Singapore High Court Orders WazirX & Zettai Pte. Ltd. to Address Creditors' Queries Amid Ongoing Moratorium Dispute

On 25 September 2024, in moratorium hearing before the High Court of Singapore, Zettai Pte. Ltd. was enquired with several questions. The proceedings, presided over by Judicial Commissioner Kristy Tan, took place via Zoom over two days, with numerous creditors raising concerns about Zettai's transparency, financial practices, and the fairness of the proposed moratorium. Zettai, which is connected to WazirX, a cryptocurrency platform implicated in a significant hack, sought a moratorium to reorganize its financial structure and address the fallout from the hack. However, creditors voiced strong opposition, casting doubt on Zettai's intentions and the legitimacy of its actions.

During the hearing, creditors accused WazirX and Zettai of manipulating the voting process related to the moratorium. Several users alleged that they had not been given the opportunity to vote against the moratorium initially, resulting in skewed results in favor of Zettai. One participant remarked that the company was "conducting the voting procedure to get it passed in their favor," further deepening suspicions about the process. Questions were also raised about the company's failure to provide a clear and fair voting structure, with many users expressing a lack of trust in the process.

In addition to concerns about the voting, the hearing also brought to light some transparency issues. Creditors demanded that Zettai and WazirX disclose proof of their reserves, which had been previously promised. Many questioned why unaffected users were being forced to bear the financial losses of those whose tokens were stolen during the hack. Some creditors went so far as to suggest that the hack may have been an inside job, which raises doubt on the company's handling of the situation. Despite WazirX's claims that the hack was a result of external interference, multiple users insisted on a full investigation to determine whether insider involvement had played a role.

Financial mismanagement of WazirX was another issue raised during the hearing. Several creditors accused WazirX of using user funds to cover legal expenses without prior authorization. One creditor pointedly asked, "Who authorized Nischal Shetty to use users' money for their purposes?" This allegation heightened the distrust many creditors already had toward the company, as it appeared that users' funds were being improperly utilized without transparency or consent. The company's financial practices were scrutinized further when creditors questioned why Zettai had not used its own profits or reserves to address the legal proceedings, instead of drawing from user funds.

In response to these concerns, the court directed Zettai to provide a detailed affidavit addressing all queries raised during the hearing. The company was given three weeks to submit this document, with the court emphasizing that all information must be made available to creditors. Only after these steps have been completed will the court decide whether to grant the moratorium.

At present, the moratorium has not yet been granted, with the court deliberating on whether the conditions of transparency and financial disclosure have been sufficiently met. The court has directed Zettai to release all relevant information before any final decision is made.

Judicial Commissioner Kristy Tan directed Zettai to submit an affidavit answering the questions rased during the proceedings on 25.09.2024 she further discussed the importance of transparency and financial disclosure, making it clear that these elements are critical to the court's final decision. The case will continue once Zettai submits its affidavit, after which the court will assess the creditors' feedback and determine whether the moratorium will be granted.

(Source: https://charltonsquantum.com/wp-content/uploads/2024/09/2024.09.26-Correspondence-from-Court-enc-hearing-chat-text.pdf)

US FinCEN & US Treasury Takes Coordinated Actions Against Illicit Russian Virtual Currency Exchanges and Cybercrime Facilitators

On 26 September 2024, the United States' Financial Crimes Enforcement Network (**FinCEN**), a division of the U.S. Department of the Treasury, passed an order whereby PM2BTC, a convertible virtual currency (**CVC**) exchanger, was officially designated as a financial institution of "primary money laundering concern" due to its involvement in illicit activities related to Russian finance. The order, issued under Section 9714(a) of the Combating Russian Money Laundering Act, prohibits all U.S. financial institutions from transmitting funds to or from PM2BTC.

On 23 September 2024, the U.S. Department of the Treasury, alongside the Department of Justice, Department of State, U.S. Secret Service, and other federal agencies, took action against Russian individuals and entities involved in large-scale cybercrime operations. These efforts were supported by international law enforcement partners, including Europol, the Netherlands Police, and the Dutch Fiscal Information and Investigation Service (**FIOD**), among others. the Office of Foreign Assets Control (**OFAC**) sanctioned Russian national Sergey Ivanov, associated with PM2BTC, and Cryptex, marking a major step in the U.S. government's mission to counter cybercrime and financial threats.

The facts underlying this case are rooted in PM2BTC's role as a CVC exchanger that operates primarily within the Russian financial ecosystem. FinCEN's investigation found that between 43% and 50% of the total transactions processed by PM2BTC were directly tied to illicit activities, including sanctions evasion, ransomware payments, fraud, and the distribution of child exploitation materials. Notably, PM2BTC processed millions in virtual currency transactions linked to major Russian ransomware groups, such as Trickbot and Conti, as well as darknet markets like Hydra and Ferum Shop. These markets facilitated the illegal exchange of goods and services, primarily through Bitcoin and other cryptocurrencies, which were then laundered through PM2BTC.

PM2BTC's operations violated provisions of the United States' Bank Secrecy Act (**BSA**), specifically concerning its failure to implement adequate Anti-Money Laundering (**AML**) and Know Your Customer (**KYC**) protocols. While PM2BTC claimed to adhere to AML standards, FinCEN's findings indicated that the company allowed anonymous transactions without proper verification of customer identities, thus facilitating the laundering of funds. This lack of compliance with KYC procedures contravened Section 5318A of the USA PATRIOT Act, which requires that all U.S. financial institutions conduct due diligence when dealing with foreign money service businesses like PM2BTC. The order also cited violations related to sanctions evasion, as PM2BTC was found to have conducted transactions with Russian entities that had been sanctioned by the Office of Foreign Assets Control (**OFAC**).

The FinCEN's authority provided by Section 9714(a) of the Combating Russian Money Laundering Act, which allows the Secretary of the Treasury to impose special measures against financial institutions deemed to be of "primary money laundering concern" when linked to Russian illicit finance. Under this provision, FinCEN exercised its power to prohibit U.S. financial institutions from engaging in the transmittal of funds involving PM2BTC. The order specifically restricts U.S. banks and financial institutions from processing any funds or cryptocurrency transactions to or from accounts associated with PM2BTC, effectively cutting off the exchanger from the U.S.

financial system. Furthermore, the order also mandates the rejection of any transactions from PM2BTC that inadvertently reach U.S. financial institutions, further insulating the U.S. financial system from the risks posed by this entity.

This regulatory action is not confined to U.S. borders; it is part of a broader transnational effort to combat money laundering and cybercrime facilitated by cryptocurrency. FinCEN worked in coordination with international agencies such as Europol, the Netherlands Police, and other foreign partners to seize PM2BTC's domains and infrastructure. The joint effort led to the shutdown of key websites associated with PM2BTC's illegal operations and the seizure of cryptocurrency assets linked to its transactions. This demonstrates the increasingly global nature of financial crime and the necessity of collaborative law enforcement efforts to tackle cross-border money laundering schemes. The international component of this case highlights the collective aim of cutting off criminal networks from the global financial ecosystem, with a particular focus on Russian-affiliated actors who exploit cryptocurrencies for illicit purposes.

(Source: https://www.fincen.gov/sites/default/files/federal_register_notices/2024-09-26/PM2BTC-Order-508.pdf, https://www.state.gov/transnational-organized-crime-rewards-program-offers-for-two-russian-nationals-and-sanctions-on-illicit-russian-virtual-currency-exchanges-and-cybercrime-facilitator/, https://www.justice.gov/opa/pr/two-russian-nationals-charged-connection-operating-billion-dollar-money-laundering-1)

US CFTC's Division of Clearing and Risk to Hold Roundtable on New and Emerging Clearing Issues

On 27 September 2024, the United States' Commodity Futures Trading Commission (**US CFTC**)'s Division of Clearing and Risk announced a public roundtable discussion to explore new and emerging issues in the clearing industry which will convene on 16 October 2024. This event will run from 9:00 a.m. to 1:00 p.m. at the US CFTC's headquarters in Washington, D.C., and will bring together a broad spectrum of participants, including representatives from derivatives clearing organizations, futures commission merchants (**FCMs**), FCM customers, end-users, custodians, proprietary traders, public interest groups, and state regulators. The goal of this roundtable is to gather expert insights and perspectives on the evolving landscape of clearing, with a particular focus on digital assets, margin requirements, and new models for clearing.

Among the key topics to be addressed are the custody and delivery of digital assets, full collateralization, the challenges of 24/7 trading, non-intermediated clearing with margin, and potential conflicts of interest within vertically-integrated entities.

The roundtable will be accessible to the public, with seating available on a first-come, first-served basis. For those unable to attend in person, the event will be live-streamed on the US CFTC's website and YouTube channel, and available via listen-only audio feed through the provided dial-in numbers. The CFTC is also accepting public comments on the issues discussed, with a submission deadline of 23 October 2024.

Digital assets are primarily built on blockchain technology, which allows for decentralized ownership, transparent transaction records, and the secure transfer of value. As the adoption of digital assets has expanded, they have presented both opportunities and challenges for regulators, particularly around issues such as custody, market integrity, and investor protection. Their unique characteristics, such as 24/7 trading and the absence of traditional intermediaries, have led to the need for updated regulatory frameworks to manage risks related to liquidity, margin requirements, and operational security.

The US CFTC's aims to ensure that the clearing industry adapts to the rapid technological advancements and new financial instruments transforming the derivatives markets. Public input from this event will help the agency address potential regulatory challenges.

(Source: https://www.cftc.gov/PressRoom/PressReleases/8985-24)

US CFTC Charges Fake Commodity Trading Platform with Fraud and Misappropriation in Scheme Targeting Asian Americans

On 27 September 2024, the United States' Commodity Futures Trading Commission (**US CFTC**) filed a civil enforcement action in the U.S. District Court for the Western District of Washington against Aipu Limited, Fidefx Investments Limited, Qian Bai, Lan Bai, and Chao Li. The CFTC's complaint alleges that, beginning on or around 6 February 2023, the defendants fraudulently solicited and misappropriated at least US $3.6 million from 32 customers through a fraudulent investment scheme. The defendants are accused of falsely offering trading in leveraged commodity and forex contracts, misappropriating customer funds, and presenting fabricated account statements through a network of fake platforms, websites, and solicitors. The fraudulent activity primarily targeted Asian American customers in the U.S., with the defendants claiming to provide high-yield returns from trading commodities and foreign currencies.

The facts of the case reveal that the defendants operated through their companies, Aipu Limited and Fidefx Investments Limited, under a common enterprise. Customers were approached via social media platforms such as WeChat, WhatsApp, and Line, where solicitors working on behalf of the defendants claimed to possess insider knowledge or specialized trading expertise that guaranteed profits of up to 30% per trade. Victims were encouraged to fund trading accounts with fiat or digital currency through the companies' websites, www.aipufx.com and www.fidefxltd.com. However, the CFTC's investigation uncovered that neither Aipu nor Fidefx had any legitimate trading accounts, and no actual trading took place on behalf of customers. Instead, the customer funds were immediately transferred to offshore accounts controlled by the defendants, where they were misappropriated.

The legal issues revolve around allegations of fraud and misappropriation under the United States' Commodity Exchange Act (**CEA**) and related US CFTC regulations. The complaint identifies violations of Sections 4b(a)(2)(A)-(C) of the CEA, which prohibit fraudulent and deceptive practices in connection with commodity trading. Additionally, the defendants are alleged to have violated Section 6(c)(1), which makes it unlawful to engage in manipulative or deceptive schemes concerning commodity futures contracts and retail forex transactions. Furthermore, the defendants did not register with the CFTC as required, nor did they use regulated futures commission merchants (**FCMs**) or retail foreign currency dealers to process customer transactions, in violation of US CFTC regulations 5.2(b)(1) and 180.1(a)(1)-(3).

The order seeks relief, including restitution for the defrauded customers, disgorgement of ill-gotten gains, and civil monetary penalties. The US CFTC is also seeking a permanent injunction to prevent further violations of the CEA by the defendants, along with trading bans to ensure the individuals and companies involved are prohibited from engaging in future commodity-related activities. The CFTC has highlighted the global nature of this fraudulent enterprise, noting that the funds were transferred to offshore entities with no connection to legitimate trading activities. The enforcement action, coordinated with international regulators and financial institutions, underscores the need for vigilance in cross-border financial fraud cases and the importance of protecting U.S. consumers from schemes involving offshore entities.

The use of digital assets and international financial networks in this case illustrates the complexity of modern financial fraud and the necessity of regulatory enforcement to maintain the integrity of the markets.

(Source: https://www.cftc.gov/PressRoom/PressReleases/8987-24, https://www.cftc.gov/media/11366/enfaipulimitedcomplaint092724/download)

Singapore High Court Grants Zettai Pte. Ltd. Four-Month Moratorium Amidst Cryptocurrency-Related Financial Crisis

On 27 September 2024, the High Court of the Republic of Singapore issued an order in the ongoing case of Zettai Pte. Ltd., a company undergoing restructuring amidst significant financial and operational challenges. This order, granted under Section 64 of the Singapore's Insolvency, Restructuring and Dissolution Act 2018 (**SG IRDA**), offers a four-month moratorium to Zettai Pte. Ltd., which effectively protects the company from any legal actions, including winding-up resolutions and other judicial proceedings initiated by creditors or stakeholders. The Honourable Judicial Commissioner Kristy Tan presided over the case, issuing a comprehensive ruling aimed at stabilizing the company while restructuring efforts are underway.

Zettai Pte. Ltd., a Singapore-based entity, found itself in a difficult position due to operational difficulties that arose when several of its cryptocurrency wallets were compromised by hackers, leading to asset losses amounting in hundreds of millions. In response to these challenges, Zettai sought protection under Singapore's IRDA, requesting a moratorium to shield itself from creditor actions while it devised a viable restructuring plan. The company argued that it needed time and space to address its financial instability, restore operations, and negotiate with creditors without the immediate threat of liquidation or legal enforcement actions.

The court's decision to grant the moratorium is a critical part of this restructuring process. It is designed to provide temporary relief to Zettai, enabling the company to continue operating while working to resolve its financial issues, including recovering from the hacking incident. The moratorium came into effect immediately and is set to last for four months, unless further extended by the court. The moratorium, issued under Section 64 of the IRDA, imposes the following restrictions and guidelines:

1. The order bars prohibits creditors or stakeholders from initiating or continuing legal proceedings, execution processes, or winding-up resolutions against Zettai without first obtaining the court's permission. This includes both local and international creditors who fall under the jurisdiction of the Singaporean courts.

2. Creditors are prohibited from taking control of or seizing any assets belonging to Zettai during this period. This prevents any forced liquidation of assets, providing the company the time to reorganize and potentially recover assets lost in the hacking incident.

3. While creditors are restrained from taking legal action, the company is allowed to pursue its own claims. Notably, Zettai retains the right to pursue any legal action or counterclaim related to proceedings initiated before 23 August 2024. This clause enables Zettai to continue its efforts in recovering assets and possibly seeking legal redress for the hacking incident.

4. As part of the court's conditions, Zettai is mandated to file affidavits that disclose crucial information about its cryptocurrency wallets, the specific wallets that were hacked, the current location of user assets, and any ongoing recovery efforts. This is aimed at ensuring transparency for both the court and Zettai's creditors.

5. Zettai must provide up-to-date management accounts and other financial records to the court during the moratorium to ensure that the company's financial status is closely monitored and that it remains accountable throughout the restructuring process.

6. Any future applications to the court that require creditor input will involve electronic voting, which must be independently verified to ensure fairness.

7. The Singapore High Court has ordered Zettai to determine the positions of its top **22 creditors** in preparation for future proceedings. This will play a critical role in any restructuring or settlement plan that Zettai may propose.

For customers and creditors, the moratorium granted by the Singapore High Court suspends their ability to take immediate action against Zettai to recover their funds or assets. This means that individuals and institutions who are owed money by the company or whose assets were impacted by the hacking incident must wait until the moratorium expires or seek special permission from the court to initiate proceedings.

For customers, particularly those whose cryptocurrency assets were compromised, Zettai's financial instability and the uncertainty surrounding the recovery of hacked assets make it unclear when or if full restitution will be possible. However, the court's requirement that Zettai provides detailed disclosures about the hacked wallets and user assets aims to reassure customers that their interests are being monitored during the moratorium.

For creditors, the moratorium creates a temporary standstill on any attempts to enforce debts or seize assets. The Singapore High Court has put safeguards in place, including financial reporting requirements, to ensure that Zettai remains transparent throughout this period. Creditors will have an opportunity to participate in the restructuring process once the company presents a plan, and their positions will be taken into account during any future applications to the court.

While the four-month moratorium offers temporary relief, the company must provide detailed disclosures, work to recover lost assets, and develop a credible restructuring plan that satisfies both the court and its creditors. If successful, Zettai may transition out of the DSS and continue operations under a revised framework.

(Source: https://charltonsquantum.com/wp-content/uploads/2024/10/2024.09.27-Sealed-Order-of-Court-OA-861-ORC-4951.pdf)

UK FCA & BoE unveils Digital Securities Sandbox: Opens Applications for Innovation and Real-World Testing

On 30 September 2024, the Bank of England and the UK Financial Conduct Authority (**UK FCA**) launched the Digital Securities Sandbox (**DSS**) and published the policy statement and guidance note on Digital Securities Sandbox operation under the UK Financial Services and Markets Act 2023 (**FSMA**). This initiative allows firms to test new financial market technologies, such as distributed ledger technology (**DLT**), in a real-world environment. The DSS provides a modified regulatory framework that supports innovation while maintaining financial stability and market integrity.

The DSS operates through a phased structure, guiding firms through four stages known as gates. Firms begin by applying for sandbox entry at Gate 1, where they start testing under regulatory supervision. In Gate 2, firms can conduct live business under set limits, such as £600 million for gilts and £900 million for corporate bonds. Gate 3 allows firms to scale their activities, increasing their limits as they meet higher regulatory standards. Finally, Gate 4 offers firms full authorization to operate outside the DSS under a new permanent regime, possibly as a Central Securities Depository (**CSD**) or other FMI.

One important point for applicants is that standalone trading venues may not qualify for sandbox entry, as the framework for these operations remains unchanged. Firms aiming to participate must demonstrate their ability to meet progressively stringent regulatory standards at each stage. Detailed guidance and application forms are available to assist firms through this process. The Digital securities sandbox ensures flexibility, with firm-specific limits and fees tailored to each stage.

The DSS provides a opportunity for firms to explore new business models and technologies while operating within a safe and controlled environment. It is expected to run until December 2028, with applications open until March 2027.

The DSS consists of four stages, each requiring firms to meet progressively higher regulatory standards before moving to the next phase. Firms entering the DSS will pass through four gates:

8. Gate 1: Application to become a sandbox entrant and begin testing – Firms apply to join the DSS, ensuring their activities and assets align with the sandbox's scope. At this stage, firms will engage with regulators but will not yet be carrying out live business activities. Testing is done under regulatory supervision.

9. Gate 2: Approval to begin live activities – Firms that pass through Gate 2 can start live business under certain limits. The Bank of England will assess whether firms meet the necessary rules for DSDs, and firms operating trading venues must comply with FCA authorization requirements. For example, the issuance limits include £600 million for gilts and £900 million for corporate bonds. Firms must pay a £40,000 fee at this stage, and annual fees are applied on a cost-recovery basis.

10. Gate 3: Scaling the business – As firms scale up, they can request to increase their operational limits, provided they meet higher regulatory standards. Specific limits will vary by firm but must stay within overall DSS limits.

11. Gate 4: Full authorization for operation outside the DSS – In this final stage, firms that successfully meet all requirements may gain full authorization to operate outside the DSS under a new permanent regime, potentially becoming a Central Securities Depository (**CSD**) or another form of FMI.

Firms may also operate as hybrid entities, combining the roles of a DSD and a trading venue. To do so, they must complete both the Bank of England's and the UK FCA's regulatory processes.

In response to feedback from 33 industry participants, the DSS has made several key adjustments, including expanding the scope to include non-GBP assets and offering greater flexibility in firm-specific limits. The capital requirement for DSDs has been reduced, and rules concerning bank guarantees and letters of credit have been simplified. The regulators have also deferred the publication of the Gate 4 rules to allow for further learning and adaptation within the sandbox.

The DSS underscores the importance of transparency and flexibility, allowing firms to innovate within a regulated environment. The initiative provides a collaborative space where firms can test new models while ensuring compliance with evolving standards, ultimately contributing to the long-term growth and success of the UK's financial markets.

(Source: https://www.fca.org.uk/news/news-stories/digital-securities-sandbox-opens-applications, https://www.fca.org.uk/firms/innovation/digital-securities-sandbox)

Crypto ATM Operator Pleads Guilty to Unregistered Network and Money Laundering Offences

On 30 September 2024, the UK Financial Conduct Authority (**UK FCA**) made a landmark announcement regarding the conviction of Olumide Osunkoya, who pleaded guilty to five significant offences at Westminster Magistrates' Court. This case marks the UK's first-ever conviction for operating an illegal network of crypto ATMs, a groundbreaking moment in the enforcement of crypto regulations. Osunkoya's network of at least 11 crypto ATMs, which processed over £2.6 million in transactions between December 2021 and September 2023, operated without FCA registration, circumventing vital anti-money laundering safeguards. The court heard how Osunkoya, undeterred by the FCA's refusal to register his business in 2021, expanded his operations in convenience stores across the UK, facilitating illegal transactions without performing due diligence or verifying the sources of funds. In addition to these regulatory breaches, he was charged with creating false documents, using a fake alias to evade detection, and possessing criminal property. His sentencing, which could result in a lengthy prison term, will take place at Southwark Crown Court, underscoring the FCA's commitment to combating financial crime in the rapidly evolving crypto sector.

The court heard that Mr. Osunkoya illegally operated at least 11 crypto ATMs across the UK, which processed over £2.6 million in transactions between 29 December 2021 and 8 September 2023. Despite being denied FCA registration in 2021, he continued expanding the network, placing the machines in local convenience stores without conducting proper customer due diligence or checking the sources of funds for transactions. Evidence presented to the court suggested that individuals engaged in money laundering and tax evasion were likely using these ATMs.

In addition to running unregistered ATMs, Mr. Osunkoya was found guilty of creating and using false documents, including the use of a false alias to evade FCA regulations. He is also charged with the possession of £19,540 in cash, suspected to be proceeds from the illegal crypto ATM operations.

The charges fall under multiple legal provisions, including UK Regulations 86 and UK Regulations 92 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (**MLRs**), which cover unregistered cryptoasset activity. Mr. Osunkoya is also facing charges under the UK's Forgery and Counterfeiting Act 1981 for the creation and use of false documents and under the UK Proceeds of Crime Act 2002 for possession of criminal property. The maximum sentences for these offences range from 2 years for unregistered operations to 10 years for forgery and 14 years for possession of criminal property.

This is the first time an individual has been prosecuted in the UK for running a network of illegal crypto ATMs. Mr. Osunkoya had previously applied for registration through his company, Gidiplus Ltd, but was refused in 2021. His actions continued despite the refusal, leading to this conviction.

(Source: https://www.fca.org.uk/news/press-releases/olumide-osunkoya-pleads-guilty-illegally-operating-crypto-atm-network)

Barclays Bank Settles with US CFTC Over Five Million Misreported Swap Transactions, Agrees to US$4 Million Penalty

On 30 September 2024, the United States' Commodity Futures Trading Commission (**US CFTC**) announced that Barclays Bank PLC had reached a settlement in response to charges of violating several key reporting regulations under the United States Commodity Exchange Act. These violations occurred between 2018 and 2023 and

involved Barclays' failure to accurately and timely report over five million swap transactions. These errors, which resulted from systemic deficiencies in Barclays' reporting systems, impacted the US CFTC's ability to assess market exposure, monitor compliance, and maintain market integrity.

The CFTC initiated proceedings under Sections 6(c) and 6(d) of the US Commodity Exchange Act, based on the bank's violations of Sections 2(a)(13) and 4r(a)(3), as well as Regulations 43.3 and 45.3-4. Barclays admitted to the findings and acknowledged that it had failed to meet the reporting standards required by the CFTC during the Relevant Period. The errors were widespread, with failures related to duplicate swap identifiers, incorrect reporting of primary economic terms, misreported timestamps, and issues with continuation data. The reporting failures not only impacted individual transactions but also posed a risk to the transparency and systemic stability of the broader financial market.

A key part of the proceedings revealed that Barclays misreported data across more than 50,000 transactions due to assigning identical identifiers to different swap transactions, effectively conflating distinct swaps. Further, 129,000 transactions involving credit and interest rate swaps were incorrectly reported with inaccurate economic terms. The US CFTC also identified 121,000 transactions where timestamps were overwritten, leading to inaccurate records. The largest issue arose with over 4.5 million transactions, where Barclays submitted stale or incorrect continuation data.

Barclays cooperated with the US CFTC throughout the investigation, voluntarily disclosing details of its reporting deficiencies and taking remedial actions to address the underlying issues. The bank's cooperation, which included providing extensive documentation and information, was considered when determining the sanctions imposed. As part of the settlement, Barclays agreed to pay a $4 million civil monetary penalty and committed to improving its internal reporting systems to prevent future violations.

Swap transactions are part of the global financial market infrastructure, and failures in reporting can obscure the real-time understanding of market risk, liquidity, and pricing. This case, involving millions of misreported transactions, highlights the importance of robust internal controls and the need for transparency in financial reporting systems.

Barclays is required to cease any further violations of the relevant sections of the US Commodity Exchange Act and continue to engage in the remedial processes it has begun. The CFTC emphasized the importance of accurate swap reporting for the protection of market participants and the overall integrity of the financial system. Barclays' settlement, including its monetary penalty and compliance commitments, marks a significant step in addressing the lapses in regulatory compliance, while also serving as a reminder of the crucial role accurate data reporting plays in maintaining fair and transparent markets.

(Source: https://www.cftc.gov/media/11401/enfbarclaysbankplcorder093024/download, https://www.cftc.gov/PressRoom/PressReleases/8988-24)

U.S. SEC Announces Departure of Enforcement Director Gurbir S. Grewal, Names Acting Leadership

On 2 October 2024, the U.S. Securities and Exchange Commission (**US SEC**) announced the resignation of Gurbir S. Grewal, Director of the Division of Enforcement, effective 11 October 2024. Following Mr. Grewal's departure, Sanjay Wadhwa, the current Deputy Director of Enforcement, will assume the role of Acting Director, while Sam Waldon, Chief Counsel of the Division, will become Acting Deputy Director.

Mr. Grewal joined the U.S. SEC in July 2021 and oversaw the Division of Enforcement through a period of active regulatory enforcement. During his tenure, he emphasised the importance of ensuring that remedies, penalties, and enforcement actions provided a deterrent effect for non-compliance. Under his leadership, the Division focused on matters such as compliance with registration provisions, whistleblower protections, and addressing deficiencies in recordkeeping across various sectors.

Mr. Grewal, before joining the U.S. SEC, served as Attorney General for the State of New Jersey and has extensive experience in law enforcement and legal practice, including roles as a U.S. Attorney and Bergen County Prosecutor. His departure will conclude his three-year service at the agency.

During his time as Director, the Enforcement Division pursued over 2,400 enforcement actions, resulting in orders of over US $20 billion in penalties, disgorgements, and funds returned to investors. Notable enforcement actions under his leadership targeted sectors including cryptocurrency markets, insider trading, and gatekeeper failures within the financial industry. The U.S. SEC brought forward numerous cases where firms failed to comply with federal securities laws, particularly in the areas of disclosure and recordkeeping.

The Division also addressed regulatory non-compliance within the cryptocurrency sector, bringing more than 100 enforcement actions against firms that failed to register with the U.S. SEC, depriving investors of required protections under federal securities laws. These actions involved penalties against some of the largest crypto asset platforms for operating without proper registration. Additionally, the Division focused on ensuring compliance in the private funds sector, addressing issues related to conflicts of interest, misrepresentation, and inadequate disclosures.

The announcement by US SEC further discussed Mr. Grewal's efforts to enhance compliance within the financial sector, particularly through encouraging firms to self-report and remediate identified issues. These measures were aimed at fostering a more robust compliance culture within regulated entities.

Sanjay Wadhwa, who will now serve as Acting Director, has over 21 years of experience at the U.S. SEC, working closely with Mr. Grewal during his time as Deputy Director. Mr. Wadhwa has led significant investigations during his tenure, focusing on insider trading, market manipulation, and institutional non-compliance. His background includes key roles in prominent enforcement actions, including those related to hedge fund misconduct and institutional trading violations.

Sam Waldon, the new Acting Deputy Director, joined the Division of Enforcement as Chief Counsel in 2022. Before joining the U.S. SEC, Mr. Waldon worked in private practice and also served as Assistant Chief Counsel for the Enforcement Division from 2010 to 2018. His experience includes advising on legal matters involving enforcement and regulatory compliance.

(Source: https://www.sec.gov/newsroom/press-releases/2024-162)

US Judge finds New California Election Deepfake Law Unconstitutional and imposed Preliminary Injuction against Assembly Bill 2839

On 2 October 2024, U.S. District Judge John A. Mendez by its order issued a preliminary injunction against California's newly enacted law, Assembly Bill 2839 (**AB 2839**), which sought to regulate the use of AI-generated deepfakes in elections. The law, signed by Governor Gavin Newsom on 17 September 2024, allowed individuals to sue for damages if AI-generated content resembling a political candidate was posted within 120 days before and 60 days after an election. This law targeted media that was deemed "materially deceptive" and harmful to the integrity of electoral processes.

The case that led to this ruling began in July 2024, when Christopher Kohls, a content creator known for his political satire under the alias "Mr. Reagan," released an AI-manipulated video mocking Vice President Kamala Harris. The video, widely circulated and shared by notable figures, including Elon Musk, generated widespread attention across social media platforms. Following this, concerns arose about the potential of AI-manipulated media or deepfakes to mislead voters and undermine political candidates.

In response to these concerns, California's legislature swiftly passed AB 2839, which sought to curb the use of such deepfakes during election periods. The law allowed for lawsuits against creators and distributors of content that could mislead voters or harm candidates through AI-altered political media. Shortly after the bill was signed into law, Kohls filed a lawsuit, challenging the constitutionality of the bill. Represented by his legal team, Kohls claimed that the law infringed on his First Amendment rights, particularly concerning his right to political satire and parody.

Kohls' lawsuit, filed on 18 September 2024, named California Attorney General Rob Bonta and Secretary of State Shirley N. Weber as defendants, seeking to block the enforcement of the new law. He argued that the legislation imposed overly broad restrictions on free speech, and its vague definitions could lead to unnecessary censorship.

Kohls' legal team contended that AB 2839 violated the First Amendment, which protects free speech, including political satire and parody. They argued that the video in question was a form of satirical expression, a category of speech that has historically been protected under the U.S. Constitution. Kohls' team emphasised that the law was overbroad, as it did not clearly distinguish between deliberately deceptive content and legitimate forms of political expression such as critique, parody, and satire.

Kohls' defense argued the chilling effect the law could have on political discourse, arguing that content creators like Kohls would be discouraged from producing satirical content for fear of potential lawsuits. The team asserted that public debate and criticism of political figures is essential in a democracy, and the law undermined this principle by threatening legal action against content creators even when the content is clearly satirical or humorous.

The State of California, represented by Attorney General Rob Bonta, defended AB 2839 as a necessary tool to protect the integrity of elections in the face of evolving technological threats, such as AI-generated deepfakes. They argued that AI-altered media poses significant risks to the democratic process, especially when it misrepresents political candidates or creates materially deceptive content that could mislead voters.

The State maintained that the law was designed to target knowingly false and malicious content, which could cause real harm during election cycles. They emphasised that the timing provisions, targeting media distributed within 120 days before and 60 days after an election, were crucial to protect voters from disinformation that could skew electoral outcomes.

State further contended that the law was aimed at minimising voter confusion and maintaining trust in the democratic process, arguing that AB 2839 was a reasonable restriction on speech to serve a compelling governmental interest, specifically the protection of election integrity.

In his ruling, Judge Mendez agreed with Kohls' argument that AB 2839 likely violated the First Amendment. While acknowledging the serious risks posed by AI-generated deepfakes, the judge concluded that the law was overly broad and did not sufficiently distinguish between deceptive content and protected speech such as satire and parody.

Judge Mendez pointed out that the U.S. legal system has a long-standing tradition of protecting political expression, including satirical and parodic content. He emphasised that while the State's concerns about election disinformation were legitimate, the First Amendment places strict limits on the government's ability to regulate speech, particularly when it concerns public debate and criticism of political figures.

The judge described the law as a "blunt tool" that served as a broad restriction rather than a narrowly tailored regulation aimed at combatting specific instances of election disinformation. He highlighted the importance of using less restrictive alternatives—such as public fact-checking, counter-speech, or targeted penalties for truly harmful disinformation—to address the issue of AI-manipulated media.

Judge Mendez ruled that the law was unconstitutional under both the First Amendment and California's free speech protections, stating that AB 2839 did not meet the required standards for content-based restrictions on speech. He granted a preliminary injunction, preventing the law from taking effect while the case proceeds.

(Source: https://charltonsquantum.com/wp-content/uploads/2024/10/preliminary-injunction-AB2839.pdf)

UK FCA Fines Starling Bank £29 Million for Failures in Financial Crime Systems and Controls

On 2 October 2024, the UK Financial Conduct Authority (**UK FCA**) issued a final notice for a fine of £28,959,426 imposed on Starling Bank Limited for failings in its financial crime controls, particularly relating to anti-money laundering (**AML**) and financial sanctions screening. The FCA's investigation revealed deficiencies in Starling's financial sanctions screening processes and its breach of an agreement to restrict account openings for high-risk customers.

Starling Bank, a digital challenger bank, saw rapid growth, expanding from 43,000 customers in 2017 to over 3.6 million in 2023. However, as its customer base expanded, the bank's financial crime controls failed to keep up. In 2021, the UK FCA conducted a review of financial crime controls across challenger banks and found concerns with Starling's anti-money laundering and sanctions screening framework.

As a result of these findings, Starling agreed to a requirement from the UK FCA not to open accounts for high-risk customers until improvements were made. Despite this, the bank continued to open over 54,000 accounts for 49,000 high-risk customers between September 2021 and November 2023, in direct violation of the UK FCA's requirement.

In January 2023, Starling discovered that since 2017, its automated sanctions screening system had only screened customers against a small portion of the financial sanctions list. This systemic issue led to multiple potential breaches of financial sanctions, which Starling has since reported to the relevant authorities.

Starling's automated system failed to screen its customers adequately against the full list of those subject to financial sanctions. This issue went undetected from 2017 to 2023, exposing the financial system to individuals who may have been involved in illegal activities or subject to sanctions. Despite agreeing to a restriction on opening accounts for high-risk customers, Starling breached this agreement and opened 54,000 accounts for 49,000 high-risk customers over a two-year period, significantly increasing the risk of financial crime. Starling reported multiple potential breaches of financial sanctions after conducting an internal review of its financial crime controls.

Therese Chambers, Joint Executive Director of Enforcement and Market Oversight at the FCA, condemned Starling's lack of controls. She stated, *"Starling's financial sanction screening controls were shockingly lax. It left the financial system wide open to criminals and those subject to sanctions. It compounded this by failing to properly comply with FCA requirements it had agreed to, which were put in place to lower the risk of Starling facilitating financial crime."*

The fine against Starling Bank serves as a clear warning to financial institutions about the importance of maintaining strong financial crime controls, especially as they grow. The failure to adequately screen customers and comply with FCA requirements not only exposed the bank to legal and reputational risks but also posed a significant threat to the integrity of the UK's financial system.

For Starling's customers, particularly those categorised as high-risk, the breaches raise concerns about the bank's ability to safeguard against financial crime. The bank's oversight in sanctions screening could have facilitated illicit financial activities, undermining trust in its systems.

Starling's breaches fall under the FCA's financial crime regulations, particularly concerning anti-money laundering (**AML**) and sanctions compliance. The UK FCA Handbook sets out clear rules for financial institutions to implement systems and controls to prevent financial crime, including the proper screening of customers against international sanctions lists. The failings identified in Starling's case represent violations of these rules, exposing the bank to financial penalties and regulatory action.

Starling's breach of UK FCA's requirement, which aimed to mitigate the risks of financial crime by restricting account openings for high-risk customers is seen as the outright breach and led to this sanction.

(Source: https://www.fca.org.uk/publication/final-notices/starling-bank-limited-2024.pdf, https://www.fca.org.uk/news/press-releases/fca-fines-starling-bank-failings-financial-crime-systems-and-controls)

Dubai AI & Web3 Festival conducted by DIFC Attracts Participations for Over 100 Countries

On 12 September 2024, under the directives of His Highness Sheikh Hamdan bin Mohammed bin Rashid Al Maktoum, Crown Prince of Dubai and Chairman of the Higher Committee for Future Technology and Digital Economy, the Dubai AI & Web3 Festival successfully concluded, drawing over 6,800 attendees from more than 100 countries. The two-day festival, organized by the Dubai AI Campus in partnership with the Dubai International Financial Centre (**DIFC**) and the Minister of State for Artificial Intelligence, Digital Economy & Remote Work Applications Office, showcased the growing commercial potential of AI and Web3 technologies.

The event basically discussed Dubai's role as a global hub for future-focused industries, attracting government officials, heads of state, business leaders, and academics from around the world. More than 100 exhibitors showcased cutting-edge technologies. A key feature of the event was the announcement of the Dubai AI Licence and the introduction of AI as a Service (**AIaaS**), both of which aim to attract AI and Web3 companies to Dubai, positioning the emirate as a leader in innovation.

The festival comes at a time when Dubai has rapidly evolved into a global center for business, finance, and emerging technologies. Arif Amiri, CEO of DIFC Authority, noted that since the establishment of DIFC 20 years ago, the center has become a pillar in supporting Dubai's economic diversification. The Dubai AI Campus, which opened during the festival, has already exceeded its initial targets, attracting over 120 firms in its first year, with plans to grow further in the coming years.

12. Dubai AI Licence: DIFC launched the first-of-its-kind Dubai AI Licence, designed to attract AI companies to Dubai, following the success of the DIFC Innovation Licence, which brought over 1,100 businesses to the financial center.

13. AI as a Service: DIFC introduced AI as a Service (**AIaaS**) to help companies assess their readiness for AI adoption, identify opportunities, develop strategies, and implement AI solutions.

14. Future Tech World Cup: The festival included the Future Tech World Cup, where AI and Web3 companies competed to showcase innovations that could revolutionize industries. The winner is set to be announced shortly.

The event attracted 6,800 delegates, including government officials, heads of state, academics, and leaders from AI and Web3 firms. 30 companies sponsored the festival, with key partners including Al Fardan Exchange, Holon, and Hyperfusion, and Dubai Chamber of Digital Economy serving as the strategic partner.

Several agreements were signed during the event, including partnerships with Dubai Civil Defence, Holon, Kearney, NayaOne, SIEF, Visa, Warba Bank, and Zurich. These collaborations aim to advance the adoption of AI and Web3 technologies in both public and private sectors.

Critical and Legal Standpoint:

The Dubai AI Licence represents a significant legal development in Dubai's regulatory framework, offering AI and Web3 companies an opportunity to operate within a favorable and secure legal environment. The introduction of AI as a Service offers an innovative tool for companies to ensure compliance with AI regulations and ethical standards while implementing AI solutions. This reflects Dubai's forward-looking approach to both technological advancement and regulatory oversight.

DIFC's role in facilitating the adoption of these technologies is supported by a strong legal and regulatory framework, ensuring that companies operating under the new licence comply with international standards for data privacy, ethics, and transparency. The legal emphasis on risk resilience, vendor management, and governance in AI deployment ensures that businesses adopting AI and Web3 technologies are well-prepared to navigate the complexities of this evolving landscape.

(Source: https://www.difc.ae/whats-on/news/dubai-ai-and-web3-festival-attracts-6800-visitors-from-over-100-countries)

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.charltonsquantum.com
www.charltonslaw.com
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596