CFTC Orders Major Penalties for Recordkeeping Supervision and Communication Failures at Truist Bank, TD Bank, and Cowen

On 14 August, 2024, the Commodity Futures Trading Commission (**CFTC**) levied significant penalties on three prominent financial institutions—Truist Bank, The Toronto Dominion Bank (**TD Bank**), and Cowen and Company—for pervasive failures related to recordkeeping, supervision, and the improper use of unapproved communication methods. These enforcement actions are a stark reminder of the critical importance of compliance with federal securities laws and CFTC regulations, with cumulative penalties reaching into the millions of dollars.

Truist Bank, a leading financial services provider based in North Carolina, has been ordered to pay a $3 million civil monetary penalty after the CFTC found that the bank failed to maintain, preserve, or produce records as required under CFTC recordkeeping regulations. The CFTC's investigation revealed that from December 2019 through the present, Truist employees, including senior executives, engaged in business-related communications using unapproved methods such as personal text messages and social media applications. These communications, which were critical to the bank's swap dealer operations, were neither monitored nor archived, in direct violation of both the bank's internal policies and federal regulatory requirements.

Despite having policies in place that broadly prohibited the use of unapproved communication methods for conducting firm business, Truist's failure to enforce these policies resulted in a significant loss of business-related communications. The firm required regular attestations from employees affirming compliance with communication policies, yet the widespread use of personal devices and applications continued unchecked. Recognizing the gravity of these lapses, Truist conducted an internal review, identified the violations, and proactively self-reported them to the CFTC. This decision to self-report, combined with the bank's substantial cooperation during the investigation, led to a reduced penalty.

TD Bank, another major player in the financial industry, faced even stiffer penalties, with the CFTC imposing a $4 million fine for its failure to diligently supervise its electronic communications surveillance system. The investigation revealed that TD Bank's oversight of its surveillance processes was severely lacking, resulting in a five-year period during which communications from hundreds of its swap dealer personnel were not properly monitored. The issue began in July 2016 when a vendor-related change disrupted the bank's automated process for ingesting communications into its surveillance tool. Instead of rectifying the problem, the bank relied on a temporary manual process, which was eventually abandoned in January 2018, leaving a substantial gap in surveillance.

This failure persisted until March 2023, by which time TD Bank had failed to surveil any new messaging platform accounts created after January 2018. The CFTC's order highlighted the bank's inadequate supervision and internal monitoring, which prevented it from detecting the surveillance gap for several years. TD Bank's failure to escalate these issues to a senior oversight body further compounded the problem. Despite these lapses, the CFTC acknowledged TD Bank's cooperation during the investigation and its ongoing remediation efforts.

In a related enforcement action, the CFTC imposed additional penalties on both TD Bank and Cowen and Company for their failure to maintain and preserve required business-related communications. TD Bank was ordered to pay an additional $75 million, while Cowen was fined $3 million. The orders revealed that both firms allowed their employees, including those at senior levels, to use unapproved communication methods for conducting business. These communications were critical to the firms' CFTC-registered activities, yet they were not maintained or preserved as required, leading to significant compliance failures.

The CFTC's investigation found that the use of unapproved communication methods, such as personal text messages, violated the firms' internal policies and federal regulations. The failure to preserve these communications meant that neither firm could promptly provide the necessary records to the CFTC when requested, severely undermining the regulatory oversight process. Furthermore, the supervisory personnel responsible for ensuring compliance with these policies were themselves found to be using unapproved methods for business-related communications, exacerbating the firms' compliance breaches.

These enforcement actions are part of a broader CFTC crackdown on non-compliance within the financial industry. Since December 2021, the CFTC has imposed over $1.2 billion in civil penalties on 24 financial institutions for similar violations of recordkeeping, supervision, and communication requirements. The significant penalties imposed on Truist Bank, TD Bank, and Cowen and Company shows the CFTC's commitment to enforcing regulatory standards and protecting the integrity of the financial markets.

(Source: https://www.cftc.gov/PressRoom/PressReleases/8945-24, https://www.cftc.gov/PressRoom/PressReleases/8944-24, https://www.cftc.gov/PressRoom/PressReleases/8943-24)

SEC Charges 26 Financial Firms $392 Million for Widespread Recordkeeping Failures

On 14 August, 2024, the Securities and Exchange Commission (**SEC**) announced a landmark enforcement action against 26 broker-dealers, investment advisers, and dually-registered entities for widespread and systemic failures in maintaining and preserving electronic communications, resulting in combined civil penalties of $392.75 million. This sweeping action, which includes major financial firms such as Ameriprise Financial Services, Edward D. Jones & Co., and RBC Capital Markets, shows the SEC's unwavering commitment to upholding the integrity of the financial markets by ensuring strict compliance with federal recordkeeping requirements.

They acknowledged that their conduct violated key recordkeeping provisions under federal securities laws. This settlement marks one of the most significant enforcement actions in recent years, reflecting the SEC's commitment to enforcing compliance with books and records requirements, which are foundational to the integrity of financial markets.

The SEC's investigation revealed that the firms and their personnel had engaged in the pervasive use of unapproved communication methods, often referred to as "off-channel communications." These methods, which include the use of personal devices and encrypted messaging apps, were not captured by the firms' official recordkeeping systems. As a result, critical communications that should have been maintained under securities laws were lost, depriving the SEC of crucial evidence during investigations.

The recordkeeping failures were not isolated incidents but were found to be systemic, involving personnel at multiple levels of authority, including senior management and supervisors. The firms were charged with violating specific recordkeeping provisions of the Securities Exchange Act and the Investment Advisers Act. Additionally, the SEC found that the firms had failed to reasonably supervise their personnel, thus failing to prevent and detect these violations.

In response to these findings, the SEC has imposed significant financial penalties on the firms, ranging from $50 million for major entities like Ameriprise and Edward Jones to $400,000 for smaller firms like Haitong International Securities (USA) Inc. Notably, three firms that self-reported their violations—Truist Securities, Cetera Advisor Networks, and Hilltop Securities—received reduced penalties, demonstrating the benefits of proactive cooperation with regulatory authorities.

Beyond the financial penalties, each firm has been ordered to cease and desist from future violations of the relevant recordkeeping provisions and has been censured. The firms have also begun implementing improvements to their compliance policies and procedures to prevent such failures from occurring in the future.

This sweeping enforcement action sets a significant precedent not only for traditional financial institutions but also for the rapidly evolving cryptocurrency industry. As crypto firms increasingly intersect with traditional financial markets, the SEC's actions serve as a stark reminder that regulatory compliance is paramount, regardless of the technology or asset class involved.

The precedent set by this case could lead to heightened scrutiny of recordkeeping practices within the crypto industry, particularly as more crypto firms seek to expand their offerings to include regulated financial products and services. The use of blockchain technology, while inherently transparent, does not absolve firms from maintaining proper records of communications and transactions, especially those conducted through off-chain methods.

The SEC's enforcement action against these 26 firms sets a precedent for the financial industry, including the emerging crypto sector, the necessity of strict adherence to regulatory standards to ensure transparency, investor protection, and the smooth functioning of markets.

(Source: https://www.sec.gov/newsroom/press-releases/2024-98)

Nasdaq ISE Withdraws Proposals to Trade Bitcoin and Ether Trust Options Following Extensive SEC Deliberations

On 14 August, 2024, the Securities and Exchange Commission (**SEC**) Chairman Gary Gensler released a statement highlighting the growing influence of artificial intelligence (**AI**) in financial markets and the potential risks it poses to investors. With AI increasingly embedded in everyday digital experiences, from search algorithms to personalized marketing, the SEC's attention has turned to its application in the financial sector, particularly in investment platforms and brokerage services.

The rise of AI has brought significant advancements in the ability to process vast amounts of data, recognize patterns, and make predictions. This technology allows companies to "narrowcast," tailoring messages, pricing, and products to individual consumers with unprecedented precision. In the financial sector, this manifests in the use of Robo-advisors and brokerage applications that rely on AI algorithms to provide personalized investment recommendations and alerts.

However, as SEC Chairman Gary Gensler pointed out in a recent address, the same AI-driven systems that enhance user experience could also introduce new risks. These algorithms, designed to predict how individuals might respond to specific prompts or offers, could potentially be manipulated to serve the financial interests of the platforms rather than the investors. Gensler raised concerns about AI's ability to detect subtle individual preferences, such as color choices or psychological triggers, which could be exploited to influence investment decisions in ways that might not align with an investor's best interests.

In a humorous twist, the video of Chairman Gensler delivering his warning appeared almost AI crafted—some joked it might have been AI-tailored itself. The lighting, the color schemes, and even the pacing of his speech seemed almost eerily optimized for maximum engagement, as if an AI system had meticulously calculated how best to hold the audience's attention. This stands on the very point Gensler was making: in a world where AI knows our preferences better than we do, the line between genuine human communication and algorithm-driven persuasion becomes increasingly blurred.

Drawing from a personal anecdote, Gensler illustrated how AI could tap into deeply ingrained preferences, such as his own aversion to the color green due to childhood experiences. He warned that AI systems, by optimizing for the platform's revenue or profit motives, could prioritize the firm's interests over those of the investor, leading to conflicts of interest. This, he cautioned, could result in investors making suboptimal financial decisions or even suffering financial harm.

The SEC is keenly aware of these potential conflicts and is actively working to address them. Gensler emphasized that regardless of whether financial advice is delivered by a human advisor or an AI-powered system, it must always serve the client's best interests. To this end, the SEC has proposed new regulations aimed at mitigating these conflicts across various investor interactions, from Robo-advisors to traditional brokers.

The proposed rule, introduced last year, seeks to ensure that AI-driven financial platforms adhere to the same standards of transparency and fairness as their human counterparts. By addressing the evolving challenges posed by AI, the SEC aims to protect investors while fostering innovation in the financial industry.

As AI continues to make waves in the financial sector, its impact is also being keenly felt in the world of cryptocurrencies and digital assets. In a market that is already known for its volatility and rapid pace of change, the integration of AI-driven algorithms presents both opportunities and challenges. On one hand, AI can provide crypto traders with sophisticated tools for market analysis, sentiment detection, and predictive modeling, potentially giving them an edge in navigating the often unpredictable crypto markets. On the other hand, the very same technology could be leveraged by platforms and exchanges to subtly influence trading behavior, possibly exacerbating market swings or encouraging trades that benefit the platform over the trader.

As decentralized finance (DeFi) platforms and crypto exchanges increasingly rely on AI to optimize user interactions and trading strategies, the potential for conflicts of interest grows. Investors must remain vigilant, ensuring that the AI tools they use are aligned with their financial goals, rather than being manipulated to serve the interests of the platform.

In this rapidly evolving landscape, the SEC's focus on AI's role in financial markets could soon extend to the crypto world, where the stakes are high and the margins for error are thin. The same principles that apply to traditional investments—transparency, fairness, and the prioritization of investor interests—must be rigorously upheld in the digital asset space to ensure that innovation does not come at the expense of investor protection.

(Source: https://www.youtube.com/watch?v=mpAE230mrdU, https://www.sec.gov/newsroom/speeches-statements/gensler-transcript-artificial-intelligence-081324)

Goldman Sachs Embraces Bitcoin ETFs Despite Previous Scepticism; Hedge Funds Bullish on Crypto Miners

On 15 August, 2024, Goldman Sachs made headlines by disclosing significant investments in Bitcoin exchange-traded funds (**ETFs**) in its quarterly 13F filing, signaling a notable shift in the bank's approach to cryptocurrency. Once a vocal skeptic of digital assets, Goldman Sachs has now become one of the largest institutional holders of Bitcoin ETFs, with positions in seven out of the 11 Bitcoin ETFs available in the U.S. market. This move, totaling $418 million in Bitcoin fund investments, marks the bank's official debut in the spot Bitcoin ETF market.

The largest portion of Goldman Sachs' Bitcoin ETF holdings is in the iShares Bitcoin Trust, where the bank has invested $238.6 million. Other substantial positions include $79.5 million in Fidelity's Bitcoin ETF, $56.1 million in Invesco Galaxy's Bitcoin ETF, and $35.1 million in Grayscale's GBTC. These investments are part of a broader trend among major financial institutions that have started to embrace cryptocurrencies, particularly following the U.S. Securities and Exchange Commission (**SEC**) opening the door for Bitcoin ETFs earlier this year.

However, Goldman Sachs' actions present a critical point of discussion within the financial community. Despite the bank's significant investments in Bitcoin ETFs, its past statements have often reflected a cautious, if not outright dismissive, attitude towards cryptocurrencies. This duality—wherein the bank once publicly expressed doubts about the viability of digital assets while simultaneously building substantial positions in crypto-related investments—raises questions about the underlying motivations and strategies of large financial institutions as they navigate the evolving landscape of digital finance.

While Goldman Sachs and other traditional financial institutions have been slow to enter the cryptocurrency market, hedge funds have taken a more aggressive approach. Millennium Management, one of the largest hedge funds globally, now holds over $1.1 billion worth of shares in various Bitcoin ETFs, making it the single largest holder of shares in BlackRock's Bitcoin fund. Other major players, such as Capula Investment Management and Point72 Asset Management, have also significantly increased their exposure to spot Bitcoin ETFs, demonstrating growing confidence in the digital asset market.

The surge in institutional interest has not been limited to Bitcoin ETFs. Hedge funds are also increasingly investing in Bitcoin mining companies, driven by the overlap between crypto mining and the energy-intensive demands of artificial intelligence (**AI**) processing. D1 Capital, for example, has acquired substantial positions in companies like Bitdeer Technologies, Iris Energy, and Hut 8, capitalizing on the convergence of AI and cryptocurrency mining operations.

Despite the influx of capital into Bitcoin and Ether ETFs, the broader crypto market remains volatile. Bitcoin's price, which reached an all-time high of over $73,000 in March, has since fallen to under $58,000. Nevertheless, the continued growth of Bitcoin ETFs, which have seen net flows of around $17.5 billion since their launch in January, suggests that institutional interest in digital assets remains strong. While public scepticism about digital assets persists, the substantial investments being made behind the scenes indicate a growing recognition of the potential long-term value and transformative impact of cryptocurrencies on the financial system.

IMF Advocates for Higher Energy Taxes on Crypto Miners and Data Centers to Curb Carbon Emissions

On 15 August, 2024, the International Monetary Fund (**IMF**) published a blog proposing significant increases in energy taxes aimed at crypto miners and artificial intelligence data centers, suggesting that such measures could play a crucial role in reducing global carbon emissions. According to a recent paper by IMF economists Shafik Hebous and Nate Vernon-Lin, raising electricity costs for these industries would not only encourage greater efficiency but also generate substantial government revenue.

The IMF's paper highlights that increasing electricity prices for crypto mining by 85% could potentially yield an additional $5.2 billion in annual global revenue while simultaneously reducing carbon emissions by 100 million tons—equivalent to the annual emissions of Belgium. The energy-intensive nature of both crypto mining and AI data processing is at the heart of this proposal, with a single Bitcoin transaction consuming as much electricity as an average person in Ghana or Pakistan uses over three years. The power demands of AI are equally staggering, with each ChatGPT query requiring ten times the energy of a standard Google search.

Hebous and Vernon-Lin further underscore that crypto mining and data centers accounted for 2% of the world's electricity consumption in 2022, a figure expected to rise to 3.5% by 2027—on par with Japan's current electricity use. This increase could push carbon emissions from these sectors to 450 million tons annually, representing 1.2% of global emissions.

The IMF's recommended strategy includes imposing targeted energy taxes that would be higher for crypto miners than for data centers, given that data centers are often located in regions with greener electricity sources. Such a tax could raise up to $18 billion annually from data centers alone. The proposal also suggests incentivizing the use of energy-efficient equipment and the adoption of less energy-intensive crypto mining methods, supported by credits for zero-emission initiatives and renewable energy certificates.

Currently, however, many crypto miners and data centers benefit from generous tax exemptions and incentives, despite their significant environmental impact and minimal contribution to employment. The IMF paper calls into question the net benefits of these special tax regimes, given the strain they place on electrical grids and the environmental harm they cause.

Several countries are beginning to adopt a more sustainable approach to managing the carbon footprint of AI and cryptocurrency industries. Nations like Sweden and Norway have introduced measures that promote renewable energy use for cryptocurrency mining. Additionally, the European Union has been exploring regulations that would impose stricter environmental standards on data centers and crypto operations.

Singapore has taken a forward-thinking and proactive stance on addressing the environmental impact of AI and cryptocurrency. The country is at the forefront of integrating sustainability into its AI and digital infrastructure strategies. As part of its National AI Strategy 2.0, Singapore emphasizes the importance of pairing AI advancements with sustainability commitments. This includes launching a $30 million fund dedicated to optimizing software design for energy efficiency and creating green-software trials to test carbon-reduction techniques in the industry.

Moreover, Singapore has developed the world's first standard to optimize the energy efficiency of data centers in tropical climates, demonstrating its leadership in sustainable technology. These initiatives are part of Singapore's broader commitment to achieving net-zero emissions by 2050 and reflect the city-state's dedication to balancing technological innovation with environmental responsibility

The IMF also emphasizes the need for cross-border coordination in implementing energy taxes. Without such cooperation, stricter regulations in one jurisdiction could merely push these energy-intensive industries to relocate to regions with more lenient standards, undermining global efforts to reduce emissions.

(Source: https://www.imf.org/en/Blogs/Articles/2024/08/15/carbon-emissions-from-ai-and-crypto-are-surging-and-tax-policy-can-help)

Google Faces $5 Million Lawsuit Over Malicious Crypto Wallet App on Play Store

On 15 August, 2024, Google has come under legal fire as it faces a $5 million lawsuit filed by Maria Vaca, who alleges that a fraudulent crypto wallet app she downloaded from the Google Play Store led to the complete loss of her savings. The lawsuit, filed in a California state court, centers on the claim that Google should be directly responsible for the security of the apps it hosts, especially those that handle sensitive financial transactions, such as cryptocurrency.

According to the lawsuit, Vaca downloaded what she believed to be a legitimate crypto wallet from the Play Store, trusting in the platform's reputation and the apparent authenticity of the app. However, shortly after installation, the app turned out to be malicious, effectively draining $5 million worth of her digital assets. The details regarding which specific crypto assets were stolen or the identity of the app have not been disclosed, leaving a cloud of uncertainty over the exact mechanisms used in the scam. This incident raises serious concerns about the adequacy of the security measures employed by Google in its app marketplace, particularly regarding the screening process for financial applications.

The relevance of this issue extends far beyond this single case, touching on the broader implications for tech giants operating in an increasingly digital and decentralized economy. As cryptocurrency continues to gain popularity and more individuals turn to digital wallets to manage their investments, the potential risks associated with these platforms grow exponentially. The security of these applications is now a matter of significant public interest, as even a single breach can result in catastrophic financial losses for users.

At the heart of the legal battle is the question of whether Google bears a legal obligation to thoroughly vet and review the authenticity of the apps available on its platform. While Google has implemented automated systems designed to screen apps for potential security threats, the effectiveness of these measures is now being called into question. The Play Store, with its vast array of applications, faces the daunting challenge of filtering out fraudulent or malicious software—a task that becomes even more complex when dealing with apps related to financial transactions, where the stakes are incredibly high.

Critics of Google's current approach argue that the tech giant's reliance on automated approval systems may not be sufficient to prevent sophisticated scams from slipping through the cracks. The rise of digital fraud has seen malicious actors develop increasingly complex methods to bypass these security protocols, leading to incidents like the one experienced by Vaca. The lawsuit underscores the need for a more rigorous and perhaps human-supervised review process, particularly for apps that could have severe financial implications for users.

This case also invites a critical examination of the broader responsibilities of digital platforms in ensuring the safety and security of their users. Should tech companies be held accountable for the apps they host, especially when those apps are found to be fraudulent? And if so, to what extent? The outcome of this lawsuit could potentially set a precedent, not only for Google but for other tech companies as well, shaping the future of digital marketplace regulations.

In addition, there are questions about whether platforms like Google Play should be more transparent about the steps they take to protect users. Should users be better informed about the risks associated with downloading certain types of apps, particularly those involving financial transactions? And should there be a stronger recourse for victims of digital fraud who have placed their trust in these platforms?

As the legal proceedings progress, the implications for Google and other tech giants could be profound. If the court sides with Vaca, it could lead to more stringent regulatory oversight of app stores and increased liability for companies that fail to protect their users from malicious software. This could also trigger a wave of similar lawsuits from others who have fallen victim to fraudulent apps, further challenging the current operational models of these platforms.

This lawsuit against Google brings to the forefront critical issues regarding digital security, user protection, and corporate responsibility in the age of cryptocurrency, and the role of platforms like Google Play in safeguarding these investments will be scrutinized more than ever.

MAS Issues 1-Year Prohibition Order Against Former HSBC Representative Mr. Aw Jun Ray Reko Corinthians

On 19 August 2024, the Monetary Authority of Singapore (**MAS**) today announced the issuance of a one-year prohibition order (**PO**) against Mr. Aw Jun Ray, Reko Corinthians, a former representative of HSBC Bank. The PO, which takes effect immediately, prohibits Mr. Aw from engaging in any financial advisory services and participating in the management, directorship, or substantial shareholding of any financial advisory or capital markets services firms regulated under the Financial Advisers Act (**FAA**) and the Securities and Futures Act (**SFA**).

The enforcement action against Mr. Aw is grounded in strict legislative provisions that govern the conduct of financial advisory professionals in Singapore. Under Section 32(2)(b) of the Financial Advisers Act 2001, any individual who, in connection with their principal's lodgment of any document, omits to state any matter or thing that results in the document being misleading in a material respect, is guilty of an offence. The penalty for such an offence includes a fine of up to $50,000. Similarly, Section 99O(2)(b) of the Securities and Futures Act 2001 outlines that individuals who fail to disclose material information, leading to a misleading document, are liable to the same penalty. These provisions are designed to ensure transparency and maintain the integrity of the financial advisory and capital markets sectors.

The MAS's decision to impose a prohibition order on Mr. Aw reflects the gravity of non-disclosure and the critical importance of honesty in the financial sector. Individuals holding positions of trust and responsibility, such as financial advisors, are expected to adhere to the highest standards of conduct. The failure to disclose material information, particularly when it pertains to criminal investigations and conditional warnings, not only undermines the trust placed in these individuals but also poses a significant risk to the integrity of the financial system.

The swift and decisive action taken by MAS serves as a stern reminder that those entrusted with the responsibility of managing financial services must operate with complete transparency. The consequences of failing to do so are severe, as demonstrated in Mr. Aw's case. This action also reinforces the message that regulatory authorities will not hesitate to remove individuals who are deemed unfit from the industry to protect the broader financial ecosystem.

The case of Mr. Aw Jun Ray Reko Corinthians highlights the imperative for all financial advisors, including those operating within the cryptocurrency space, to remain vigilant and fully aware of their legal obligations. As the regulatory landscape continues to adapt to new financial technologies, crypto financial advisors must ensure they operate within the bounds of the law, maintaining transparency and integrity in all their dealings. Violations of trust and non-disclosure can lead to severe repercussions, not only for the individual advisor but also for the broader financial ecosystem. Upholding the highest standards of conduct is essential to preserving the credibility and trust that clients place in financial advisors, particularly in the complex and often volatile world of cryptocurrency.

The prohibition order against Mr. Aw Jun Ray Reko Corinthians establishes the important role of regulatory oversight in maintaining the trust and integrity of Singapore's financial and ensures that the highest standards of honesty and transparency are upheld, thereby safeguarding the interests of all stakeholders within the industry.

(Source: https://www.mas.gov.sg/regulation/enforcement/enforcement-actions/2024/mas-issues-prohibition-orders-against-mr-aw-jun-ray-reko-corinthians)

MAS Issues Nine-Year Prohibition Order Against Former OCBC Bank Representative Mr. Hoi Wei Kit

On 19 August 2024, in a decisive move to uphold the integrity of Singapore's financial advisory sector, the Monetary Authority of Singapore (**MAS**) issued a nine-year prohibition order (**PO**) against Mr. Hoi Wei Kit, a former representative of OCBC Bank. This action follows Mr. Hoi's conviction for multiple serious offences under the Penal Code (**PC**) and the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (**CDSA**). The prohibition order is a clear message from MAS about its zero-tolerance policy towards financial misconduct, particularly when it involves a breach of trust with clients.

The criminal activities committed by Mr. Hoi occurred between October 2017 and January 2018, during which he defrauded five OCBC customers. By falsely claiming that OCBC was offering time deposit accounts, Mr. Hoi induced these customers to sign up for these non-existent products. He then transferred a total of $170,000 from their accounts into his own personal bank account. Such fraudulent behavior not only violated the trust of the affected customers but also severely tarnished the reputation of the financial institution he represented.

Following an investigation, Mr. Hoi was convicted on 21 February 2022 of five counts of cheating under section 420 of the Penal Code, one count of acquiring benefits from criminal conduct under section 47(1)(c) of the CDSA, and one count of giving false information to a public servant. In addition to these convictions, the court took into consideration three additional counts of cheating and ten counts of acquiring benefits from criminal conduct during sentencing. Consequently, Mr. Hoi was sentenced to 30 months of imprisonment, reflecting the severity of his crimes.

Given these convictions, the MAS deemed Mr. Hoi unfit to continue in any capacity within the financial advisory sector. The prohibition order, which took effect immediately, bars Mr. Hoi from providing any financial advisory services, participating in the management, acting as a director, or becoming a substantial shareholder of any financial advisory firm under the Financial Advisers Act (**FAA**) for a period of nine years. This prohibition underscores the MAS's commitment to ensuring that only individuals who meet the highest standards of integrity and professionalism are allowed to operate within the financial services industry.

The legal basis for Mr. Hoi's conviction and the subsequent prohibition order lies in the provisions of the Penal Code and the CDSA. Section 420 of the Penal Code addresses the crime of cheating. It stipulates that any individual who dishonestly induces a person to deliver property, alter, or destroy a valuable security, or any document that is signed or sealed and capable of being converted into a valuable security, can be punished with imprisonment for a term that may extend to 10 years, and may also be liable to a fine. This section underscores the seriousness with which the law views deceitful acts that result in financial loss or damage to another person.

Moreover, section 47(1) of the CDS Act criminalizes actions related to the concealment, disguise, conversion, or transfer of property that represents benefits from criminal conduct. It also criminalizes the acquisition, possession, or use of such property. These provisions are designed to prevent individuals from benefiting from illicit gains and to ensure that the financial system is not used as a vehicle for money laundering or other illegal activities.

The case of Mr. Hoi serves as a crucial reminder to all financial advisers and professionals within the financial services industry of the importance of maintaining the highest standards of honesty and integrity. The MAS's stringent regulatory measures are in place to ensure that those entrusted with public confidence are fit and proper to carry out their duties. The prohibition order against Mr. Hoi is not just a punitive measure but also a preventive one, aimed at protecting the public and maintaining the credibility of Singapore's financial system.

(Source: https://www.mas.gov.sg/regulation/enforcement/enforcement-actions/2024/mas-issues-prohibition-order-against-mr-hoi-wei-kit)

MAS Reaffirms Commitment to Safeguarding Customer Data Amid Growing Concerns

On 19 August 2024, in response to public concerns regarding the protection of national data by financial institutions (**FIs**), the Monetary Authority of Singapore (**MAS**) issued a strong statement reaffirming its commitment to the stringent safeguarding of customer data. This follows a letter by Dr. Pei Sai Fan, published in Lianhe Zaobao on 10 August 2024, which called for enhanced protection of citizens' data held by insurance companies and other financial institutions.

MAS has made it clear that all FIs, including insurers, must implement robust and comprehensive IT security measures to ensure that customer data is shielded from unauthorized access or disclosure. This directive is part of the broader regulatory framework under which MAS-licensed insurers operate, ensuring that they maintain sound IT security policies as a fundamental aspect of their operations. These requirements are in line with Singapore's commitment to maintaining a secure and resilient financial ecosystem, particularly in an era where cyber threats are increasingly sophisticated and pervasive.

Moreover, MAS emphasized that all FIs in Singapore are also bound by the Personal Data Protection Act (**PDPA**). The PDPA governs the collection, use, and disclosure of personal data, stipulating that such data should only be utilized for legitimate purposes recognized under the Act or with the explicit consent of the individual. This legal framework applies uniformly to data, regardless of whether it is held by Singaporean or foreign institutions, thereby ensuring that all customer data is afforded the same level of protection. MAS reiterated that firm action will be taken against any entity or individual found in violation of these stringent data protection laws and regulations.

MAS's firm stance on data protection is a positive step toward strengthening public trust in Singapore's financial system. By enforcing strict data protection regulations, MAS not only safeguards the interests of consumers but also enhances the overall integrity of the financial sector. This commitment to data security is critical in maintaining Singapore's reputation as a leading global financial hub, where the protection of customer information is paramount. The proactive measures outlined by MAS are likely to encourage other financial institutions to adopt even more rigorous data protection protocols, ensuring that Singapore remains at the forefront of financial security and innovation.

However, while MAS's response is commendable, there remains a need for continuous vigilance and adaptation to new and emerging threats. The rapidly evolving landscape of cybercrime means that financial institutions must not only comply with existing regulations but also anticipate and respond to potential future risks. It is crucial that MAS continues to update and refine its guidelines to address these challenges effectively. Additionally, there should be greater transparency in how data protection measures are enforced and monitored, ensuring that breaches are swiftly detected and addressed. The recent concerns raised by Dr. Pei Sai Fan highlight the importance of an ongoing dialogue between regulators, financial institutions, and the public to ensure that data protection remains a top priority.

In the midst of the digital economy expansion, the protection of personal data will become increasingly critical. MAS's decisive actions in this regard are a vital component of Singapore's broader strategy to secure its financial infrastructure against cyber threats and maintain the confidence of its citizens and the global financial community.

(Source: https://www.mas.gov.sg/news/letters-to-editor/2024/response-to-letter—protect-citizens-data-held-by-income)

CFTC Orders Houston-Based Firm and Managing Member to Pay Over $520,000 for Forex Fraud Violations

On 20 August, 2024, in a decisive move against financial fraud, the Commodity Futures Trading Commission (**CFTC**) announced that it has issued an order against Get Money Tradez LLC (**GMT**) and its managing member, Jeffrey Carmon, Jr., based in Houston, Texas, requiring them to pay more than $520,000 in penalties and restitution. The CFTC found that the respondents had engaged in a fraudulent scheme involving two forex trading pools, soliciting nearly $1 million from 19 unsuspecting participants, only to misappropriate significant portions of those funds for personal use.

The investigation revealed that from July 2021 to the present, GMT and Carmon solicited $950,000 from the public under false pretenses. Carmon falsely claimed to be a highly successful forex trader, despite suffering net losses in 17 out of 19 months from January 2020 to July 2021. Instead of fulfilling his promises to invest the pool participants' funds, Carmon misappropriated at least $113,000, which he diverted for personal expenses including payments to the IRS, restaurant bills, and retail purchases. The order also uncovered that the respondents had commingled pool funds and failed to register as required under the Commodity Exchange Act (**CEA**).

As part of the settlement, the CFTC has ordered GMT and Carmon to jointly pay $262,000 in restitution to the defrauded participants and an additional $262,000 as a civil monetary penalty. The respondents are also permanently banned from trading in CFTC-regulated markets and from registering with the CFTC, effectively removing them from the financial industry.

This ruling by the CFTC sends a powerful message to the financial industry: fraudulent activities will not be tolerated, and those who engage in such behavior will face severe consequences. The swift action by the CFTC not only holds the wrongdoers accountable but also demonstrates the Commission's commitment to protecting the integrity of the financial markets and safeguarding the public from fraudulent schemes. This outcome underscores the importance of regulatory oversight in maintaining trust and transparency in financial markets.

While the CFTC's actions are commendable, the case of Get Money Tradez LLC highlights ongoing challenges in protecting investors from sophisticated fraud schemes. Despite stringent regulations, fraudulent operators continue to exploit gaps in the system, often leaving victims with little recourse. The fact that Carmon was able to operate his fraudulent scheme for several years raises concerns about the effectiveness of current regulatory mechanisms in detecting and preventing such activities. Moreover, the CFTC's caution that orders requiring restitution may not result in the full recovery of lost funds underscores the limitations of post-facto enforcement actions.

This case also has significant implications for the cryptocurrency and digital asset markets, where similar fraudulent schemes have been known to occur. The CFTC's enforcement action against Get Money Tradez LLC serves as a stark reminder that the principles of investor protection and regulatory compliance apply equally to traditional and digital financial markets. As the popularity of cryptocurrency trading continues to surge, so too does the risk of encountering bad actors who exploit the relatively unregulated nature of the space. This ruling highlights the necessity for cryptocurrency investors to exercise caution and due diligence, ensuring that any trading platforms or investment opportunities they engage with are properly registered and regulated. The case reinforces the importance of a robust regulatory framework to prevent fraud in the crypto market and protect investors from significant financial losses.

Investors are urged to remain vigilant and conduct thorough due diligence before committing funds, particularly in high-risk areas like forex trading. The CFTC's advisory on forex fraud provides critical information on identifying potential scams, and the public is encouraged to utilize resources like the NFA BASIC system to verify the registration status of individuals and firms. By working together, regulators, financial institutions, and investors can strengthen the defenses against financial fraud and enhance the overall security of the financial system.

(Source: https://www.cftc.gov/PressRoom/PressReleases/8947-24)

SEC Issues 2025 Fee Adjustment Order: Impacts Traditional and Crypto Securities Alike

On 20 August, 2024, the U.S. Securities and Exchange Commission (**SEC**) issued a crucial order adjusting the registration fee rates for fiscal year 2025, set to take effect on 1 October, 2024. This adjustment, detailed in the "Order Making Fiscal Year 2025 Annual Adjustments to Registration Fee Rates," establishes a new fee rate of $153.10 per million dollars of securities registered. The SEC's move reflects its ongoing commitment to ensuring that the fees collected are aligned with the regulatory demands of overseeing a dynamic and complex financial market. This change underscores the SEC's role in maintaining a robust regulatory framework that protects investors and ensures market integrity.

The impact of this rule change will be felt across a broad spectrum of companies that are required to register their securities with the SEC. The adjusted fee rate will inevitably lead to increased costs for these companies as they prepare to issue new securities. For large corporations issuing substantial amounts of securities, this could

mean a significant increase in their regulatory costs. However, this change is not merely a financial burden; it represents the SEC's strategy to keep pace with the growth and evolution of the securities market, ensuring that it has the resources needed to effectively regulate and enforce compliance.

The SEC's process for adjusting the fee rate for fiscal year 2025 is careful and detailed, ensuring that the fees collected match the agency's regulatory needs. The SEC begins by estimating the total value of securities expected to be registered during the year, which for 2025 is a significant $5.65 trillion. To set the new fee rate, the SEC divides its target fee collection amount of $864.7 million by this estimate, arriving at a rate of $153.10 per million dollars of securities registered. This rate is applied to all relevant securities registrations. This calculation helps the SEC meet its fee collection goals while providing companies with a clear and predictable cost structure. By adjusting these rates annually, based on market conditions and forecasts, the SEC ensures it can continue to regulate the securities market effectively.

For companies in the crypto space, particularly those whose tokens or digital assets have been classified as securities by the SEC, this rule change carries specific implications. Crypto and DeFi entities that are required to register their tokens as securities will now be subject to the same adjusted fee rates as traditional financial entities. This adds another layer of regulatory compliance and financial responsibility for these companies, many of which are still navigating the complexities of U.S. securities laws. The increased fees may also influence how these companies structure their offerings, potentially leading to more strategic decisions about when and how to register their tokens with the SEC.

SEC's adjustment to registration fees for fiscal year 2025 is a significant shift that will affect both traditional financial institutions and emerging crypto, NFTs and DeFi enetities. As the regulatory landscape evolves, especially with the growing intersection of digital assets and securities law, companies across the board will need to adapt to these changes to remain compliant and competitive. This adjustment is not just a procedural update; it is a reflection of the SEC's proactive stance in regulating an increasingly digital and decentralized financial world.

(Source: https://www.sec.gov/files/rules/other/2024/33-11299.pdf)

SEC Approves Updated PCAOB Audit Standards: Addresses Auditor Responsibilities, Contributory Liability Rule, and Technology Use

On 20 August, 2024, the Securities and Exchange Commission (**SEC**) announced the approval of updates to the Public Company Accounting Oversight Board (**PCAOB**) audit standards, which will take effect for audits of financial statements beginning from 15 December, 2024. These changes include updated standards on general auditor responsibilities, the incorporation of technology-assisted analysis in audit procedures, and a significant amendment to the PCAOB's contributory liability rule for associated persons of audit firms.

The SEC has endorsed the PCAOB's new AS 1000, "General Responsibilities of the Auditor in Conducting an Audit," which modernizes and consolidates the principles governing an auditor's duties. This standard emphasizes the auditor's role in safeguarding investor interests by ensuring the issuance of accurate, independent reports. It also reinforces the need for auditors to exercise due professional care, scepticism, and judgment while adhering to stringent ethics and independence rules.

Additionally, the SEC approved amendments to AS 1105, "Audit Evidence," and AS 2301, "The Auditor's Response to the Risks of Material Misstatement," to address the use of technology-assisted data analysis tools in audits. These updates clarify the auditor's responsibilities when deploying advanced analytical tools, ensuring that technology use aligns with the overarching goals of transparency and accuracy in financial reporting.

The amendment to PCAOB Rule 3502, which will become effective in 60 days, shifts the standard for contributory liability from recklessness to negligence. This adjustment aligns the rule with other negligence-based professional conduct standards, ensuring that individuals within audit firms are held accountable if their actions directly and substantially contribute to the firm's violations.

The adoption of the updated PCAOB audit standards and the amendment to the contributory liability rule carry significant implications for the cryptocurrency industry, which has long been under scrutiny for its opaque financial practices and the complexity of auditing digital assets. As cryptocurrencies and blockchain technology become more integrated into mainstream finance, the need for rigorous and transparent auditing processes

becomes ever more critical. The SEC's approval of these changes signals a clear intent to bring the auditing of crypto entities up to par with traditional financial institutions, ensuring that the same level of scrutiny and accountability applies across the board.

One of the most notable aspects of the updated standards is the explicit inclusion of technology-assisted analysis in audit procedures. For the cryptocurrency sector, which is inherently digital and data-driven, this development is particularly important. Blockchain transactions, while public, are often complex and involve multiple layers of cryptographic verification. The ability of auditors to effectively use advanced data analytics and technology-assisted tools will be crucial in navigating these complexities, allowing for more accurate and efficient audits of crypto assets and transactions.

Furthermore, as cryptocurrency firms often operate on a global scale with decentralized structures, the shift towards a negligence-based standard for contributory liability under Rule 3502, raises the stakes for individuals within audit firms who are responsible for the oversight of crypto-related audits. Auditors and associated persons will need to exercise heightened diligence in their review and reporting processes, as any lapses that directly and substantially contribute to regulatory violations could now result in legal and professional consequences under the revised standards.

The implications of these updates extend beyond just compliance; they are likely to influence how cryptocurrency firms approach their internal controls and financial reporting practices. With the SEC and PCAOB emphasizing the importance of ethical conduct, professional scepticism, and the use of cutting-edge technology, crypto firms will need to ensure that their financial statements are prepared and audited with the highest standards of accuracy and transparency.

Moreover, the enhanced auditing standards could also play a role in legitimizing the cryptocurrency market in the eyes of institutional investors. As these investors increasingly seek exposure to digital assets, they demand the same level of assurance and reliability that they receive from traditional financial products. By enforcing stricter audit standards, the SEC and PCAOB are helping to create a more trustworthy environment for investing in cryptocurrencies, which could lead to increased capital inflows and further integration of digital assets into the global financial system.

SEC Commissioner Hester M. Peirce expressed significant concerns regarding the PCAOB's recent proposals, which include shifting the contributory liability standard from recklessness to negligence and updating audit standards for technology-assisted data analysis. Peirce cautioned that the change to a negligence-based standard could unintentionally lower audit quality and deter talent from entering the auditing profession. She emphasized that this shift appears driven more by a desire for aggressive enforcement than by a clear necessity and could exacerbate existing challenges in the audit industry, such as market concentration and the departure of seasoned auditors.

While supporting the modernization of audit standards to incorporate technology, Peirce voiced reservations about the potential costs and burdens these amendments could impose on auditors and their clients. She stressed the need for clear implementation guidance and raised questions about the PCAOB's authority to make such changes. Peirce's concerns highlight the importance of balancing rigorous enforcement with the need to maintain a collaborative and efficient audit process, as the SEC moves forward with these regulatory updates.

SEC Chairman Gary Gensler expressed strong support for the final amendments aimed at modernizing audit standards through the integration of technology-assisted data analysis. He highlighted that these updates are crucial in keeping pace with the rapid advancements in technology, particularly in the finance sector. Gensler emphasized that the amendments will provide auditors with a robust, risk-based framework to ensure the reliability of large data sets, enhance the quality and quantity of audit evidence, and update essential audit procedures. He praised the PCAOB for its efforts in revising these standards, which are vital for maintaining the integrity and effectiveness of the audit process in the 21st century.

(Source: https://www.sec.gov/newsroom/press-releases/2024-100, https://www.sec.gov/newsroom/speeches-statements/peirce-remarks-pcaob-082024, https://www.sec.gov/newsroom/speeches-statements/gensler-remarks-pcaob-technology-082024)

Tether Announces Launch of Dirham-Pegged Stablecoin

On 20 August 2024, Tether, the world's largest issuer of stablecoins, announced the launch of a new stablecoin pegged to the UAE Dirham (**AED**). This development marks a strategic collaboration between Tether and UAE-based companies, Phoenix Group and Green Acorn Investments, aiming to introduce a digital asset fully backed by liquid reserves within the UAE. The new Dirham-pegged stablecoin is expected to play a pivotal role in enhancing financial transactions both within the UAE and on an international scale, offering a secure and efficient means for trade, remittances, and reducing transaction costs.

The introduction of this stablecoin comes as the UAE continues to assert itself as a global economic hub, particularly in the areas of blockchain and digital assets. With the implementation of the UAE Central Bank's Payment Token Services Regulation (**PTRS**), the Dirham-pegged stablecoin will be launched under a robust regulatory framework designed to ensure its stability and security. The PTRS framework mandates that businesses and vendors in the UAE only accept crypto payments for goods and services if they are backed by Dirham-pegged tokens. This regulation, coupled with the requirement for foreign payment token issuers to register with the Central Bank and maintain 100% of their reserves in cash, underscores the UAE's commitment to fostering a secure and transparent digital financial ecosystem.

The launch of Tether's Dirham-pegged stablecoin aligns with the UAE's broader vision of becoming a leader in digital finance, a vision further supported by the establishment of the Virtual Asset Regulatory Authority (**VARA**) and the emergence of Dubai and Abu Dhabi as global innovation hubs for crypto assets and blockchain technology. As the UAE continues to embrace digital technologies, this new stablecoin is poised to become a critical tool for businesses and individuals seeking to leverage the benefits of the Dirham in the rapidly evolving digital economy.

The regulatory environment surrounding stablecoins has been evolving rapidly as governments and financial authorities around the world recognize the need to ensure the stability and security of these digital assets. The UAE's Payment Token Services Regulation is a prime example of how nations are proactively creating frameworks to manage and regulate the issuance and use of stablecoins. Such regulations are crucial in preventing the misuse of stablecoins for illicit activities and ensuring that they are backed by sufficient reserves. The global financial community is closely monitoring these developments, as the regulation of stablecoins will play a pivotal role in their broader acceptance and integration into the mainstream financial system.

From a user and trader perspective, stablecoins have gained significant traction due to their ability to provide the stability of traditional currencies combined with the benefits of blockchain technology. Consumers and businesses alike appreciate the lower transaction costs, faster settlement times, and the ability to conduct cross-border transactions without the need for intermediaries. However, there are also concerns about the transparency of reserve holdings and the potential risks associated with the centralization of stablecoin issuers. Despite these concerns, the demand for stablecoins continues to grow, particularly in regions like the UAE, where there is a strong appetite for innovative financial solutions.

While the rise of stablecoins presents numerous advantages, it also raises several critical issues that need to be addressed. The centralization of stablecoin issuance by a few major players, such as Tether, poses risks related to market dominance and the potential for systemic instability if these issuers were to face financial difficulties. Additionally, the rapid proliferation of stablecoins has sparked debates about their impact on monetary sovereignty, especially in emerging markets where these digital assets could potentially compete with national currencies.

Despite the challenges, the future of stablecoins appears bright, with significant potential to revolutionize the way we conduct financial transactions. As more countries and regions, like the UAE, embrace stablecoins, these digital assets could become a cornerstone of the global financial infrastructure.

SEC Updates Definition of Qualifying Venture Capital Funds with Inflation Adjustment

On 21 August, 2024, the Securities and Exchange Commission (**SEC**) adopted a rule change affecting the venture capital industry by adjusting the dollar threshold required for a fund to qualify as a "qualifying venture capital fund" under the Investment Company Act of 1940. This adjustment is mandated by the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 (**EGRRCPA**), which requires the SEC to update this threshold every five years to account for inflation. Crypto venture capital funds, like their traditional counterparts, bene-

fit from being classified as "qualifying venture capital funds" under the Investment Company Act because this classification exempts them from the more stringent regulations that apply to investment companies. The SEC's proposed rule adjustment to increase the threshold for qualifying venture capital funds to $12 million is a positive development for the crypto industry. It provides more flexibility for crypto venture capital funds to raise and manage capital, encouraging continued investment in blockchain innovation.

The core purpose of the proposed rule is to adjust the financial threshold that determines whether a venture capital fund qualifies for an exemption from the more rigorous regulatory framework imposed on "investment companies" under the Investment Company Act of 1940. This exemption is critical for venture capital funds, as it allows them to operate with greater flexibility, free from the burdensome registration and compliance requirements that apply to traditional investment companies. The original threshold, set at $10 million in aggregate capital contributions and uncalled committed capital, was established under the EGRRCPA. However, this threshold is subject to inflationary pressures, which over time could erode its effectiveness. To counteract this, the EGRRCPA mandates that the SEC adjusts this figure every five years to reflect changes in the economic environment, specifically inflation.

It proposes to increase the current threshold from $10 million to $12 million. This adjustment is based on the inflation rate as measured by the Personal Consumption Expenditures Chain-Type Price Index (**PCE Index**), which the SEC has chosen as the most appropriate measure for this purpose. The PCE Index is a comprehensive indicator of inflation that captures price changes across a wide range of goods and services within the U.S. economy. By comparing the PCE Index values from May 2018, when the original threshold was set, to December 2023, the SEC determined that a $2 million increase in the threshold is necessary to maintain its intended impact.

The rule also establishes a structured process for future inflation adjustments. Every five years, the SEC will reassess the threshold using the PCE Index, ensuring that it continues to reflect current economic conditions. This approach not only provides a clear methodology for future adjustments but also offers stability and predictability for venture capital funds, allowing them to plan their capital-raising activities with greater certainty.

The proposed rule will become effective 30 days after its publication in the Federal Register. This timeline gives venture capital funds a short window to adapt to the new threshold, but the SEC expects the impact to be minimal, as the adjustment is primarily a technical correction to account for inflation.

From an economic perspective, the document includes an analysis of the potential impacts of the rule change. The SEC anticipates that the rule will have a minimal overall effect on the venture capital market, primarily benefiting funds that are currently near the $10 million threshold. For these funds, the increased threshold provides additional room to raise capital while still qualifying for the regulatory exemption. This is particularly important for smaller and emerging venture capital funds, which rely on this exemption to operate more flexibly and efficiently.

However, the document also acknowledges that the overall effect on the venture capital market is likely to be limited, as relatively few funds operate precisely at this threshold. The inflation adjustment is designed to maintain the status quo rather than to expand or contract the scope of the exemption significantly.

The proposed rule is designed to be minimally disruptive to the existing regulatory framework. It does not introduce new reporting or compliance requirements, nor does it impose additional burdens on venture capital funds. The SEC has certified that the rule will not have a significant economic impact on a substantial number of small entities, further underscoring its targeted nature.

In keeping with its standard rulemaking process, the SEC is inviting public comments on the proposal. Stakeholders are encouraged to provide feedback on various aspects of the rule, including the choice of the PCE Index as the measure for inflation adjustments, the estimated number of funds that will be affected by the change, and the broader economic implications of the adjustment. This feedback will help the SEC refine the rule and ensure that it effectively serves its intended purpose.

(Source: https://www.sec.gov/newsroom/press-releases/2024-102, https://www.federalregister.gov/documents/2024/02/21/2024-03436/qualifying-venture-capital-funds-inflation-adjustment)

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