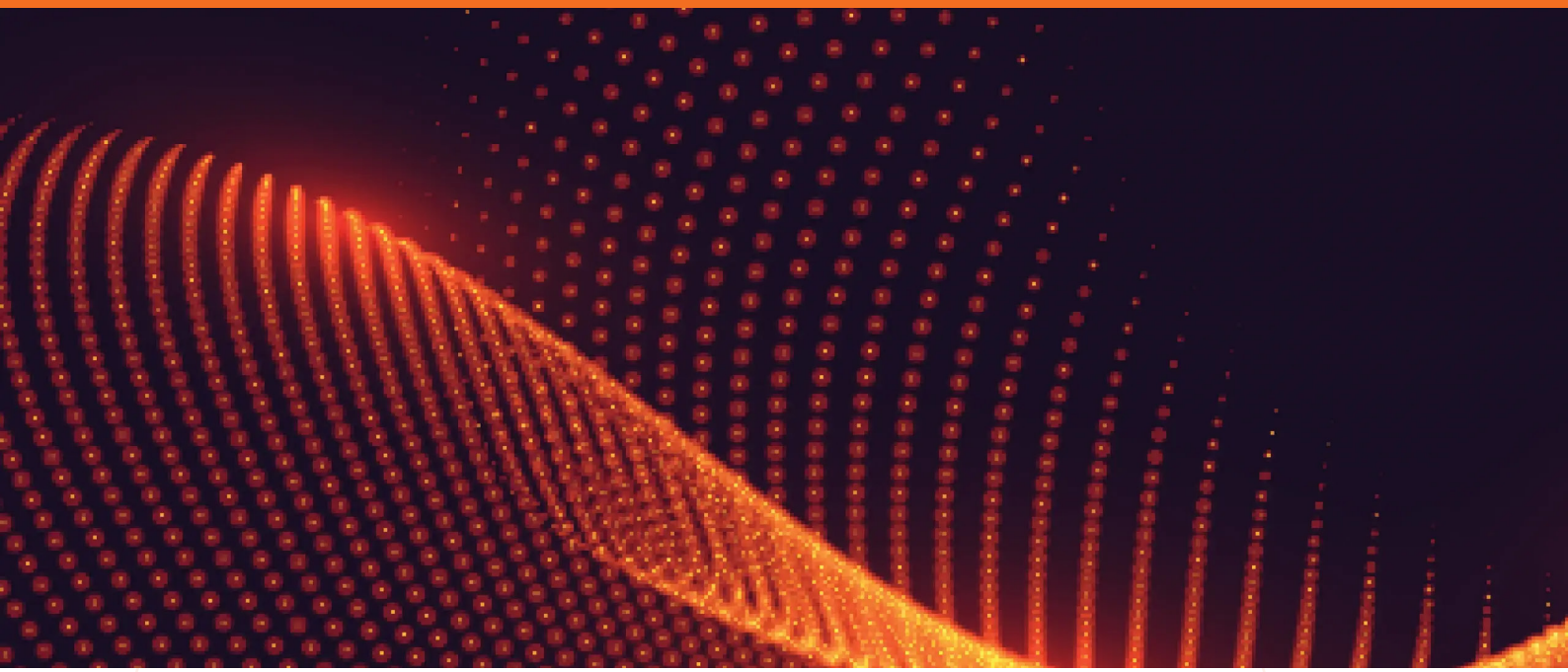

US CFTC Enforcement Division Issues Prediction Markets Advisory

On 25 February 2026, the US CFTC's Division of Enforcement issued an Advisory on Enforcement Authority over Event Contracts following the public release of two enforcement cases involving misuse of non public information and fraud on KalshiEX, a designated contract market.

The cases involved a political candidate who traded on his own candidacy and a YouTube channel editor who traded on advance knowledge of video content. Kalshi imposed financial penalties and suspensions in both cases and reported them to the US CFTC. The Division's advisory emphasised that while Kalshi's internal enforcement programme handled these matters, the US CFTC retains full authority to police illegal trading practices on any DCM. Prohibited practices include misappropriation of confidential information in breach of a pre existing duty of trust and confidence, pre arranged non competitive trading and wash sales. These alleged acts violated prohibitions on misappropriation of confidential information in breach of a pre-existing duty of trust and confidence to the source of the information (commonly known as "insider trading") pursuant to Section 6(c)(1) of United States Commodity and Exchange Act, and Regulation 180.1(a)(1) and (3).

The advisory establishes an enforcement baseline for prediction market integrity and reaffirms that DCMs are self regulatory organisations with independent obligations to maintain audit trails, conduct surveillance and enforce rules against prohibited practices. The advisory also serves notice to market participants that the US CFTC will investigate and prosecute violations where federal action is warranted.

(Source: https://www.cftc.gov/PressRoom/PressReleases/9185-26)

US CFTC Reaffirms Exclusive Jurisdiction Over Prediction Markets in Ninth Circuit Filing

On 17 February 2026, the US CFTC filed an amicus curiae brief in the U.S. Court of Appeals for the Ninth Circuit in *North American Derivatives Exchange, Inc. v. State of Nevada*. The brief confirmed the US CFTC's exclusive jurisdiction over U.S. commodity derivatives markets, including event contract markets commonly referred to as prediction markets.

The filing marked the US CFTC's first formal judicial intervention in the rapidly expanding litigation over the legal status of event contracts and prediction markets. The brief advanced three interlocking legal arguments: event contracts are swaps under United States Commodity and Exchange Act (CEA Act) under Section 1a(47), the CEA Act field preempts state gambling laws as applied to DCM listed event contracts and state gambling laws are independently preempted under conflict preemption doctrine. The US CFTC has filed only eight amicus briefs since the turn of the century, therefore the rarity and importance of this intervention.

The amicus filing intervention in support of Crypto.com's appeal against the Nevada Gaming Control Board, US CFTC has placed its institutional authority behind the position that federally regulated event contracts preempt state gaming enforcement. Multiple appellate courts, including the Third, Fourth and Ninth Circuits, are expected to address this jurisdictional question in the coming months.

US CFTC Chairman Michael S. Selig stated: *"CFTC-registered exchanges have faced an onslaught of lawsuits seeking to limit Americans' access to event contracts and undermine the CFTC's sole regulatory jurisdiction over prediction markets. This power grab ignores the law and decades of precedent. Event contracts allow businesses and individuals to hedge event-driven risks, enable investors to manage portfolio exposure, and provide the public with information about the outcome of future events. These products are commodity derivatives and squarely within the CFTC's regulatory remit. As I've said before, the CFTC has the expertise and responsibility to defend its exclusive jurisdiction over commodity derivatives, and that's exactly what we'll do."*

(Source: https://www.cftc.gov/PressRoom/PressReleases/9183-26)

US DOJ Sentences Paxful Holdings Inc. to USD 4 Million Criminal Penalty for Travel Act and Bank Secrecy Act Violations

On 11 February 2026, the US DOJ announced that Paxful Holdings Inc., an online peer to peer virtual currency trading platform, was sentenced to pay a criminal penalty of USD 4 million. The sentence followed Paxful's guilty plea to conspiracies to promote illegal activities, violate the United States Bank Secrecy Act (BSA) and knowingly transmit funds derived from criminal offences.

Paxful pleaded guilty in December 2025 in the United States District Court for the Eastern District of California. Court documents established that the appropriate criminal penalty was USD 112,500,000. The US DOJ determined that Paxful lacked the ability to pay more than USD 4 million. Paxful received a 25 per cent reduction from the bottom of the applicable sentencing guidelines fine range. This credit reflected cooperation with the investigation and remedial measures undertaken.

From 1 January 2017 to 2 September 2019, Paxful facilitated more than 26.7 million trades. These totalled nearly USD 3 billion in value. The platform collected more than USD 29.7 million in revenue during this period.

Paxful knowingly transferred virtual currency on behalf of customers, including Backpage, an online advertising platform for illicit activities. Between December 2015 and December 2022, the collaboration with Backpage and a similar site caused nearly USD 17 million in Bitcoin to be transferred from the Paxful wallet to these platforms. Paxful earned at least USD 2.7 million in profits from this arrangement. Paxful's founders described this revenue stream as the "Backpage Effect."

From July 2015 to June 2019, Paxful marketed itself as a platform that did not require KYC information. It allowed customers to open accounts and trade without sufficient identification. The company presented fabricated AML policies to third parties. It failed to file a single suspicious activity report (SAR) until November 2019, despite awareness of criminal activity on its platform.

"Paxful profited from moving money for criminals that it attracted by touting its lack of anti-money laundering controls and failure to comply with applicable money-laundering laws, all while knowing that these criminals were engaged in fraud, extortion, and other illicit activities," said US DOJ Assistant Attorney General A. Tysen Duva.

On 8 July 2024, Paxful co founder and former Chief Technology Officer Artur Schaback pleaded guilty to conspiracy to fail to maintain an effective AML programme. The guilty plea was part of a coordinated resolution with the Financial Crimes Enforcement Network (FinCEN), which assessed a USD 3.5 million civil money penalty.

Homeland Security Investigations (HSI) and IRS CI investigated the case.

Compliance Considerations for Peer to Peer Virtual Currency Platforms

The Paxful conviction is among the most consequential enforcement actions against a peer to peer cryptocurrency exchange. It establishes that platforms which market non compliance as a feature face criminal liability. The absence of KYC procedures, SAR filing obligations and independent AML auditing collectively constituted the basis for conviction. VASPs operating in any jurisdiction must ensure BSA compliance, FinCEN registration and robust transaction monitoring. The case further illustrates that profit derived from facilitating criminal transactions, even through third party integrations, attracts direct criminal liability for the platform entity itself.

(Source: https://www.justice.gov/opa/pr/virtual-asset-trading-platform-sentenced-violating-travel-act-and-other-federal-criminal)

US DOJ Sentences Fugitive Daren Li to 20 Years for USD 73 Million Cryptocurrency Investment Fraud

On 9 February 2026, the US DOJ Criminal Division announced the sentencing of Daren Li, aged 42, to 20 years in federal prison. The court also imposed three years of supervised release. Li had pleaded guilty on 12 November 2024 in the Central District of California to conspiring to launder funds obtained from victims through cryptocurrency scams and related fraud.

The conspiracy operated from scam centres based in the Kingdom of Cambodia. Co conspirators contacted victims through unsolicited social media messages, telephone calls, text messages and online dating platforms. They built trust through fabricated professional or romantic relationships. Victims were then directed to deposit funds into spoofed cryptocurrency trading platforms designed to resemble legitimate exchanges.

In certain instances, the group posed as technical support representatives. They induced victims to transfer funds via wire transfers or cryptocurrency platforms to resolve fabricated computer related issues.

Li admitted that at least USD 73.6 million in victim funds were deposited into bank accounts under his control and that of co conspirators. Of this total, USD 59.8 million was routed through accounts of United States based shell companies before being converted into virtual assets to obscure the funds' origin.

US DOJ Assistant Attorney General A. Tysen Duva of the Criminal Division stated *"As part of an international cryptocurrency investment scam, Daren Li and his co-conspirators laundered over $73 million dollars stolen from American victims,"* said

Eight co conspirators have pleaded guilty to date. Li is the first defendant sentenced who was directly involved in the receipt of victim funds.

The United States Secret Service (USSS) Global Investigative Operations Center led the investigation. The Homeland Security Investigations El Camino Real Financial Crimes Task Force, Customs and Border Protection National Targeting Center, United States Department of State Diplomatic Security Service, Dominican National Police and United States Marshals Service provided assistance.

This sentencing is a deterrent against the pig butchering operations. These schemes exploit social engineering tactics and spoofed digital asset platforms. Virtual asset and crypto asset service providers may consider implementing robust transaction monitoring protocols, and may consider to flag high volume deposits from unknown sources routed through shell entities.

(Source: https://www.justice.gov/opa/pr/man-sentenced-20-years-prison-role-73-million-global-cryptocurrency-investment-scam)

Artificial Intelligence and the Future of Investment Management: Director of Division of Investment Management, US SEC's Vision for the Future of Investment Management

On 3 February 2026, the Brian Daly, Director, Division of Investment Management, United States Securities and Exchange Commission addressed a speech titled Artificial Intelligence and the Future of Investment Management at the Investment Company Institute Winter Board Meeting. The Division of Investment Management acknowledged uneven AI adoption across advisers and funds. Liability exposure was identified as a primary concern. The US SEC invited direct engagement from market participants deploying AI systems. It also raised the possibility of using large language models to modernise investor disclosures.

The Director stated that *"the greatest impediment to a more widespread adoption of AI is liability concerns."* He recognised enforcement sensitivity but indicated that such concerns should not be insurmountable. The Division of Investment Management drew parallels with earlier technological shifts, including algorithmic trading.

The Director envisioned artificial intelligence as a generational regulatory challenge, as he compared current AI concerns to earlier debates around electronic delivery and algorithmic trading. The speech acknowledged that existing rules were drafted in a pre-digital environment. Particular emphasis was placed on the Books and Records Rule and e delivery frameworks.

The Division indicated reluctance to rush into prescriptive AI rulemaking. Instead, it encouraged industry dialogue, pilot programmes, and potential no action engagement. The speech also explored whether large language models could replace static PDF prospectuses with interactive AI agents trained on official disclosure documents.

The US SEC also questioned whether AI driven disclosure tools could replace static PDF prospectuses. It asked whether such systems would constitute marketing, require investment adviser registration, and how they would be supervised.

AI deployment does not dilute fiduciary duties under the United States Investment Advisers Act. Supervisory controls, audit trails, model governance and disclosure consistency remain central. AI chat interfaces, automated portfolio tools may trigger marketing rule, registration and record retention obligations.

The Division encouraged firms to seek dialogue, including no action engagement where appropriate. The posture is engagement driven, but fiduciary standards remain intact, and Innovation in Autonomous systems must be governed.

(Source: https://www.sec.gov/newsroom/speeches-statements/daly-020326-artificial-intelligence-future-investment-management)

US DOJ Completes USD 400 Million Forfeiture of Assets Tied to Helix Darknet Bitcoin Mixer

On 29 January 2026, the US DOJ announced the completion of a forfeiture exceeding USD 400 million in seized cryptocurrencies, real estate and monetary assets. These assets were tied to the operation of Helix, a darknet cryptocurrency mixing service.

Judge Beryl A. Howell of the United States District Court for the District of Columbia entered the final order of forfeiture on 21 January 2026. The order declared the assets forfeited to the United States government.

Helix operated from 2014 to 2017 as a Bitcoin tumbling service. It blended cryptocurrency from multiple users and routed funds through a series of transactions. The service was designed to obscure the sources, destinations and ownership of funds. Helix processed at least 354,468 Bitcoin, valued at approximately USD 300 million at the time of transactions. Investigators traced tens of millions of dollars from darknet marketplaces through the mixer.

Larry Dean Harmon of Akron, Ohio, operated Helix. He also ran Grams, a darknet search engine. Harmon pleaded guilty in August 2021 to conspiracy to commit money laundering. He was sentenced in November 2024 to 36 months in prison, three years of supervised release, a forfeiture money judgement and forfeiture of seized property.

Helix integrated its Application Programming Interface (API) directly with major darknet marketplaces. This enabled seamless Bitcoin withdrawal through the mixer from illegal drug markets.

The IRS Criminal Investigation (IRS CI) Cyber Crimes Unit and FBI Washington Field Office investigated the case. The US DOJ Office of International Affairs and the United States Attorney's Office for the Northern District of Ohio provided assistance.

Compliance Considerations on Cryptocurrency Mixers and Privacy Tools

The Helix forfeiture is one of the largest asset recoveries connected to a cryptocurrency mixing service globally, specifically against mixing platforms that fail to implement AML and KYC controls. The case sets a precedent for regulatory treatment of privacy enhancing crypto tools. It signals that platforms designed to obscure transaction trails face criminal liability irrespective of when the illicit activity took place. Since 2020, the US DOJ Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) has secured over 180 cybercrime convictions and court orders returning more than USD 350 million to victims. The forfeiture demonstrates that blockchain forensics and international cooperation can trace and recover crypto assets years after the underlying offences.

(Source: https://www.justice.gov/opa/pr/government-forfeits-over-400m-assets-tied-helix-darknet-cryptocurrency-mixer)

US DOJ Sentences Chinese National Jingliang Su to 46 Months for USD 36.9 Million Digital Asset Laundering Conspiracy

On 27 January 2026, the US DOJ announced the sentencing of Chinese national Jingliang Su, aged 45, to 46 months in federal prison. The United States District Judge R. Gary Klausner of the Central District of California also ordered Su to pay USD 26,867,242.44 in restitution.

Su pleaded guilty in June 2025 to one count of conspiracy to operate an illegal money transmitting business. He was part of an international criminal network that targeted 174 American victims through a digital asset investment conspiracy. The operation was similarly carried out from scam centres in Cambodia.

Overseas co conspirators contacted US victims through unsolicited social media interactions, telephone calls, text messages and online dating services. They gained victims' trust and directed them to spoofed cryptocurrency trading platforms. Victim funds were then laundered through United States shell companies, international bank accounts and digital asset wallets.

Su joined a shell company known as Axis Digital and participated in crypto conversions and fund transfers. Co conspirators Jose Somarriba and ShengSheng He each pleaded guilty to conspiracy to operate an unlicensed money transmitting business. He was sentenced to 51 months and Somarriba to 36 months in prison.

"This defendant and his co-conspirators scammed 174 Americans out of their hard-earned money, in the digital age, criminals have found new ways to weaponize the internet for fraud. The Criminal Division and its law enforcement partners have continued to evolve and caught large-scale scammers, who target people through their phones, social media, and fake internet sites, steal from them, and then move their money through cryptocurrency and wire transfers outside of the United States." said US DOJ Assistant Attorney General A. Tysen Duva.

Su has been in federal custody since December 2024. Eight co conspirators have pleaded guilty to date.

The USSS Global Investigative Operations Center investigated the case, with assistance from Homeland Security Investigations, Customs and Border Protection, United States Department of State Diplomatic Security Service and Dominican National Police.

Regulatory Considerations on Stablecoin Conversion and Shell Entity Structures

The Su case discusses the use of stablecoin conversion and shell entities as laundering conduits. Compliance officers at cryptocurrency exchanges must enhance know your customer (KYC) protocols for corporate accounts. Entities with opaque beneficial ownership structures should consider triggering enhanced due diligence (EDD) procedures. The Financial Action Task Force (FATF) identified in its 2025 report that USD 51 billion of illicit on chain activity was directly linked to fraud and scam schemes in 2024, with stablecoins increasingly used as a medium for laundering.

(Source: https://www.justice.gov/opa/pr/chinese-national-sentenced-prison-role-crypto-scam-targeting-americans)

US CFTC Chairman Selig Announces Senior Staff Appointments

Between 20 January and 2 March 2026, US CFTC appointed senior staff members. On 20 January 2026, the first round of staff appointments was announced. On 26 January 2026, Alex Titus was named Chief Advisor to the Chairman. Titus joined the US CFTC from the White House Council of Economic Advisers, where he served as Chief of Staff under Chairman Stephen Miran.

On 23 February 2026, four additional appointments were announced. These included Brooke Nethercott as Director of the Office of Public Affairs, Emma Johnston as Senior Agriculture Advisor, Meghan Tente as Senior Advisor and Elizabeth Mastrogiacomo as Senior Advisor. On 2 March 2026, Chairman Selig announced three further senior appointments: David I. Miller as Director of Enforcement, Mel Gunewardena as Director of the Office of International Affairs and Senior Markets Advisor, and Alan Brubaker as Director of the Office of Legislative and Intergovernmental Affairs.

(Source: https://www.cftc.gov/PressRoom/PressReleases/9184-26 / https://www.cftc.gov/PressRoom/PressReleases/9187-26 / https://www.cftc.gov/PressRoom/PressReleases/9169-26)

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