GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation 2026

Eighth Edition

Contributing Editor:
Josias N. Dewey
Holland & Knight LLP

WSBA WALL STREET BLOCKCHAIN ALLIANCE

glg Global Legal Group

TABLE OF CONTENTS

Jurisdiction Chapters

Dark patterns leading to the dark forest – the next frontier of crypto enforcement?

Sarah Chen
Gregory Strong
Frank Weigand

Cahill Gordon & Reindel LLP

Over the past several months, there has been a sea change in terms of the regulatory approach to blockchain and digital assets in the United States. The U.S. Securities and Exchange Commission (the "SEC") has done a veritable 180-degree turn and has gone from a "regulation by enforcement" posture, in which it viewed most digital assets as unregistered securities, to setting up a crypto task force to facilitate digital asset activities and set clear boundaries as to when the securities laws apply to those activities. This new approach to blockchain and digital assets has resulted in the SEC ending a number of high-profile active enforcement actions and closing many more enforcement investigations involving digital assets. There is a growing recognition that digital assets are not themselves securities and, unless sold in investment contract transactions, are not subject to U.S. securities laws.[1]

Similarly, the U.S. Commodity Futures Trading Commission (the "CFTC") has recently sought to facilitate digital asset activities in the U.S. through various published guidance and statements to the market.[2]

Although the federal securities and commodities regulators have taken a more relaxed approach towards digital assets, federal and state consumer protection agencies may seek to fill the void. Consumer protection laws, which are flexible and principles-based, can be used to address activities involving digital assets to ensure that users engaging with blockchain networks, blockchain-based technology, and digital assets are protected.

A recent trend in consumer protection involves enforcement actions based on "dark patterns" – deceptive user interfaces that manipulate consumers into actions they might not otherwise take. The Federal Trade Commission (the "FTC") has aggressively pursued dark patterns cases in the last several years and state attorneys general have coordinated to bring or resolve multistate investigations involving the use of dark patterns.

Although we have not yet seen an enforcement action in the digital assets space alleging consumer protection violations involving dark patterns, it may only be a matter of time. The steps involved in processing digital asset transactions are complex and largely opaque to users, who typically rely heavily on technology tools to construct, broadcast, and execute such transactions. Couple that with surface-level disclosures regarding how those technology tools function and the potential for unfairness or deception is significant. Where federal securities regulators under the previous administration attempted to regulate this type of digital asset activity through aggressive enforcement on the theory it was

securities activity, that is no longer the case. However, if consumers are harmed when they participate in digital asset transactions, consumer protection regulators could very well step in and fill the gap.

This chapter explores the potential application of consumer protection laws and dark patterns to user interfaces (whether a website or mobile application) that facilitate consumer activity involving digital assets and practical considerations that may help to address these issues.

The dark forest

Ethereum has famously been described as a "dark forest" – an environment where advanced predators kill anything they detect.[3] The Ethereum mempool, where pending transactions wait to be added to a block, is the primary hunting ground where bots scan the dark forest for transactions that they can profit from.

While Ethereum has changed significantly since it was first described as a dark forest in 2020, the manner in which transactions on Ethereum, and other blockchain networks, are constructed, routed, executed and added to blocks, and the manner in which blocks are added to the chain, is complex. For the average user of Ethereum, and many other blockchain networks, transaction construction, routing, execution, validation, ordering, and block building is a mystery. But how transactions are routed, executed, validated, ordered and added to blocks, and how blocks are added to the chain, can materially affect users.

Transaction initiation, routing, and execution on Ethereum

Typical blockchain users rely on a variety of tools designed to allow them to interact with blockchain networks. We will use Ethereum to illustrate how these interactions work. Many other account-based blockchain networks function in a similar manner.

Wallet software is an important tool that facilitates user interactions with blockchain networks through an interface or application that allows users to manage their Ethereum account. There are two types of accounts on Ethereum – externally owned accounts ("EOAs") and contract accounts.[4] An EOA on Ethereum is controlled by a private key, while a contract account is a smart contract deployed to Ethereum that is controlled by code. Both an EOA and a contract account can receive, hold and send ETH or other tokens and interact with other smart contracts deployed to Ethereum. EOA wallet software is designed to (i) maintain private keys securely in the case of EOAs, (ii) view and manage token balances associated with the account, (iii) construct and initiate transactions, and (iv) translate user instructions given through a user interface into function calls in a format that can be broadcast to and understood by network participants. Smart contract-based wallet software allows for programmability that can enhance security, facilitate gas payments for transactions in a variety of ways by bundling multiple actions into a single transaction, and provide other security and user experience benefits. A new hybrid called a "Smart EOA" was introduced recently in EIP-7702[5] and allows EOAs to use smart contract account features through a delegation process. As this is a new standard, its use has been limited so far and is not addressed in this chapter – instead we focus on EOA and smart contract accounts and wallet software.

There are three types of transactions on Ethereum that users can initiate through wallet software: (i) transfers from one EOA to another EOA; (ii) transactions in which an EOA deploys a contract; and (iii) transactions that involve an interaction with a deployed contract through a function call.[6] EOA wallet software allows users to build these transactions by inputting the details of the intended transaction, which may include variables such as (i) recipient's address or address of the contract with which the user intends to interact, (ii) the asset to be transferred, (iii) data for the contract, and (iv) setting a cap on the gas for the transaction. Once a transaction is built, EOA wallet software allows users to sign the transaction object with their private key for submission to the network.

Smart contract wallet software works differently and allows users to construct a transaction in the form of a user operation. User operations are different from transaction objects in that a user operation can

contain multiple instructions and smart contract calls. To do this, user operations contain additional data fields to allow the user operation to be verified and signed; user operations are sent to an alternate mempool where bundlers package user operations into transactions for inclusion in a block, bundlers use their own EOAs to sign transactions consisting of bundles of user operations for submission to an entrypoint contract, and the entrypoint contract authenticates each user operation in the bundle and executes each user operation for transactions that have been authenticated.

What happens once these transactions are built and signed is usually opaque to users, as the transactions move from the wallet software[7] and enter the dark forest when submitted to the network.

Typically, transactions broadcast to the network, using wallet software through a decentralized application or a backend server, will be received by a node on the network. Network transactions are validated by one of many nodes running the network client software and participating in transaction validation. The receiving node will confirm that the transaction is well formed, there is a valid signature, the account has enough ETH to pay for gas, and the nonce for the transaction has not already been used. Once validated, the node generates a transaction hash that identifies the transaction and it is added to the mempool and broadcast to other nodes where validators can choose to include the transaction in an upcoming block. It can take anywhere from seconds to many hours for unconfirmed transactions in the mempool to be included in a block. How long this takes depends on factors like the level of network usage and the gas fee paid in connection with the transaction.

When a transaction is included in a block, it is executed by the Ethereum Virtual Machine (the "EVM"). This results in a change in the state of the ledger as ETH balances associated with accounts involved in the transaction will change when gas is paid and other state changes reflecting the transaction details will also be recorded in the ledger.

On Ethereum, the process of block building is complex and evolving. This process has evolved, in part, to address the issues that gave rise to the "dark forest" description noted above. Unconfirmed transactions in the mempool are observable to validator nodes in the network and to other network participants using specialized tools. In addition, these unconfirmed transactions in the mempool can now be observed using certain block explorer tools that are publicly available. This allows those participants to see unconfirmed transactions and take action based on the expected result of those transactions once confirmed and added to a block. These actions typically involve extracting value known as maximal extracted value or "MEV" (not to be confused with "EVM"). For instance, if a transaction is observed in the mempool that provides for an arbitrage opportunity, an MEV searcher may submit a bundle of transactions directly to a block builder designed to take advantage of the arbitrage opportunity presented and extract value from that opportunity.

One of the ways that block building on Ethereum has evolved to address MEV is through proposer builder separation. In this system, which is not an official "enshrined" component of the Ethereum network but is implemented in certain ancillary validation systems, such as MEV-Boost built by Flashbots,[8] block building is separated from block validation and finalization. Block builders construct blocks by including transactions using MEV opportunities to maximize value and submit these blocks to validators. Validators then assess blocks submitted by many block builders and will select the highest-paying block to add to the blockchain. This process prioritizes adding transactions that will generate more fees or that present MEV opportunities to blocks than lower-value transactions.

Although the above descriptions are very high level, and could be described in considerably more detail, the primary point is that the process of constructing, broadcasting, authenticating, and adding transactions to blocks is complex and involves many different participants. Against this backdrop, we discuss the concept of dark patterns from a legal perspective.

Dark patterns

So-called "dark patterns" are manipulative or deceptive interface designs that steer, trap, or confuse consumers. The FTC defines "dark patterns" as design tricks that manipulate consumers.[9] Some examples of dark patterns include obstructive cancellation, misdirection, burying key terms, drip fees, and steering data-sharing via biased defaults and confusing flows. "Dark patterns can be found in a variety of industries and contexts, including ecommerce, cookie consent banners, children's apps, subscription sales, and more."[10]

In recent years, both federal and state consumer protection regulators have brought enforcement actions alleging violations of consumer protection laws in connection with online flows that use dark patterns to trick consumers. The general theory is that dark patterns constitute unfair, deceptive, or abusive acts or practices ("UDAAP") that are prohibited by federal and state consumer protection laws.

The Federal Trade Commission and dark patterns

In 2023, the FTC filed an enforcement action against Amazon alleging that it "duped millions of consumers into unknowingly enrolling in its Amazon Prime service" using "manipulative, coercive, or deceptive user-interface designs known as 'dark patterns'."[11] The FTC further alleged that (i) Amazon leveraged manipulative user interface designs – so-called "dark patterns" – in its checkout and enrollment flows to steer or trick consumers into opting into Prime, often obscuring the full cost, renewal terms, or subscription conditions, and (ii) Amazon sometimes collected consumers' payment information (e.g., stored credit or debit card credentials) before clearly presenting the full Prime terms, effectively locking in consumers before they could decline.

The FTC also alleged that Amazon made cancellation of Prime subscriptions unduly complex, burdensome, and confusing. Internally, Amazon referred to the cancellation flow as "Iliad," a multi-step process requiring consumers to affirm their desire to cancel across multiple pages, including prompts intended to dissuade cancellation. According to the amended complaint, Amazon consciously rejected internal proposals to streamline or simplify cancellation – decisions motivated by revenue retention rather than customer convenience. The FTC further asserted that Amazon's misrepresentations and user interface choices harmed consumers: some were enrolled in Prime without awareness; while others began cancellation but abandoned it mid-process. The amended complaint sought injunctive relief, changes to Amazon's user interface and disclosure practices, and redress to affected consumers. The FTC claims these practices constitute violations of Section 5 of the Federal Trade Commission Act of 1914 (the "FTC Act") (for unfair or deceptive acts) and the Restore Online Shoppers' Confidence Act ("ROSCA"), which mandates clear disclosures and explicit consumer consent for recurring billing.

The FTC action against Amazon was recently settled for $2.5 billion.[12]

The FTC Act prohibits unfair and deceptive acts or practices in commerce.[13] An act or practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition" is unfair.[14] A consumer injury must be substantial, and not merely trivial or speculative, in order to trigger application of the FTC Act.[15] Typically, substantial injury involves financial harm, and in some cases, health and safety risks can also constitute substantial injury.[16] Subjective types of harm are usually not enough to cause substantial injury.[17]

The injury must also not be outweighed by countervailing benefits to consumers. For example, if providing complex disclosures to consumers regarding a product would cause the price of the product to increase, the consumer benefit of a lower price would be weighed against the potential harm associated with the lack of disclosure and the net effect considered. Finally, the injury cannot be reasonably avoidable by consumers.

Most actions alleging violations of Section 5 of the FTC Act are brought to address seller behavior that impedes individual consumer choice and decision-making.[18] An act or practice that unjustifiably interferes with the ability of consumers to make their own free and informed purchasing decisions will usually be unfair for purposes of the FTC Act.[19]

Misrepresentations or deceptive omissions of material fact also constitute deceptive acts or practices prohibited by Section 5(a).[20]

There are three elements of deception cases considered by the FTC:

1) a misrepresentation, omission, or practice exists that is likely to mislead the consumer;
2) the act or practice must be viewed through the lens of a reasonable consumer; and
3) the misrepresentation, omission, or practice must be material.[21]

A misrepresentation requires a representation that is likely to mislead and is material to the reasonable consumer.[22] An omission of material information occurs when information necessary to prevent a claim, practice, or sale from being misleading is not disclosed.[23]

Practices related to marketing and point of sale representations can also be deceptive practices if they are likely to mislead consumers. Situations in which inaccurate or incomplete information is provided to prospective consumers in marketing materials or at the point of sale may constitute deceptive practices. The act or practice must be viewed through the objective lens of the reasonable consumer.[24]

As noted in the Amazon example above, use of dark patterns has been alleged to be both unfair and deceptive by the FTC.

The Consumer Financial Protection Bureau and dark patterns

The Consumer Financial Protection Bureau (the "CFPB") is another federal regulatory agency created to protect consumers by enforcing the Consumer Financial Protection Act (the "CFPA"). The CFPA prohibits UDAAP with respect to financial products offered primarily for consumer use by "covered persons."[25]

The scope of CFPB authority is narrow and there are several key restrictions. First, the UDAAP provisions of the CFPA[26] only apply to financial products offered or provided for consumer use. The definition of "financial product or service" contains a list of products that fall within the definition and which are subject to CFPB jurisdiction when offered to consumers. The list is long and includes "engaging in deposit-taking activities, transmitting or exchanging funds, or otherwise acting as a custodian of funds or any financial instrument for use by or on behalf of a consumer", for example.

Second, CFPB jurisdiction is limited to providers of consumer financial products or services. The term "covered person" means: (a) any person that engages in offering or providing a consumer financial product or service; and (b) any affiliate of a person described in point (a) if such affiliate acts as a service provider to such person. The term "service provider" means any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service, including a person who: (i) participates in designing, operating, or maintaining the consumer financial product or service; or (ii) processes transactions relating to the consumer financial product or service (other than unknowingly or incidentally transmitting or processing financial data in a manner that such data is undifferentiated from other types of data of the same form as the person transmits or processes).

In addition, any person who knowingly or recklessly substantially assists a violation by a covered person or service provider will also be in violation of the CFPA to the same extent as the primary violator.[27]

Third, there are exceptions for persons registered with or regulated by the SEC or CFTC, provided that they are acting within the scope of their registered or regulated capacity.[28]

The standards for unfair and deceptive acts and practices under the FTC Act inform the standards in the CFPA for those terms.[29] Under the CFPA, an act or practice is unfair when it "causes or is likely to cause consumers substantial injury that is not reasonably avoidable and if the substantial injury is not outweighed by countervailing benefits to consumers or to competition."[30] This unfairness standard is almost identical to the FTC Act unfairness standard. The same is true for deception, which is detailed as follows under the CFPA: (1) an act or practice that misleads or is likely to mislead consumers; (2) the consumer's interpretation is reasonable under the circumstances, and (3) the misleading act is material.[31]

The UDAAP provisions also prohibit abusive acts or practices. The CFPB released a policy statement[32] addressing what constitutes an abusive act or practice, being one that (i) obscures important features of a product or service, or (ii) leverages circumstances – such as gaps in understanding, unequal bargaining power, or consumer reliance – to take unreasonable advantage of consumers.[33]

The CFPB sued TransUnion in 2022, alleging that the company used a variety of "dark patterns to trick people into recurring payments and to make it difficult to cancel them."[34] The CFPB alleged that TransUnion collected credit card information from consumers seeking a free annual credit report that appeared to be part of an identity verification, but then used that credit card information to charge consumers on a recurring monthly basis who had unknowingly made a purchase by clicking a deceptive button in the enrollment process.[35] When consumers sought to cancel these subscriptions, the process to do so was intentionally made difficult by TransUnion according to the complaint.[36] The CFPB charged TransUnion with engaging in deceptive acts or practices in connection with these dark patterns.[37]

Since filing this lawsuit in 2022, the CFPB has been overhauled and the TransUnion lawsuit was voluntarily dismissed by a joint stipulation of the parties filed on February 25, 2025 in the Northern District of Illinois where the case was pending.[38] Given the CFPB overhaul, it is not expected that the CFPB under the current administration will be active with respect to digital assets or enforcement related to digital assets.

State attorneys general

State consumer protection statutes typically provide state attorneys general with broad authority to address unfair and deceptive acts and practices. These statutes generally apply to consumer transactions and are principles-based. This means they are flexible, adaptable, and can be applied to address alleged misconduct in a variety of contexts. State consumer protection statutes, for example, have been used to address unfair debt collection, misrepresentations regarding financial products, and off-label marketing of drugs. Many of these cases have been pursued by multistate coalitions of state attorneys general offices.

State attorneys general also have the authority to enforce the UDAAP and certain other provisions of the CFPA.[39] This allows them to bring enforcement actions in federal court whenever they evidence that a UDAAP has occurred in their jurisdiction in connection with the offer of a consumer financial product or service.[40] In certain states, enforcement authority under the CFPA and the ability to enforce the UDAAP provisions extends state attorney general consumer protection authority beyond what is provided for under state laws alone. The CFPB and state attorneys general have brought several coordinated enforcement actions alleging CFPA violations. In January of this year, prior to the change in administration, the CFPB published a Roadmap for State Consumer Protection[41] setting out steps that state consumer protection regulators could consider. This roadmap compliments prior CFPB guidance on state attorney general enforcement of the CFPA.[42]

In addition, a multistate coalition of 40 state attorneys general recently reached agreements with Google to resolve allegations that Google engaged in deceptive and unfair acts and practices in connection with its location tracking, location history, and location settings.[43] The findings in the Assurances of Voluntary Compliance,[44] or similar settlement agreements entered into with specific state attorneys general, detailed the myriad ways that Google tracked users' locations and revealed that even if a user wanted to disable location tracking through a particular means, it would be tracked through other means.[45] For example, when a user turned off "Location History," Google would still track that user's location through

other Google account settings such as Web & App Activity or Google location services.[46] By using dark patterns, including various levels of location tracking, Google made it nearly impossible for users to stop their location from being tracked according to the Assurances of Voluntary Compliance or other settlement agreements.[47]

Dark patterns and the dark forest

Blockchain transactions are complex. From transaction initiation to execution, there are a number of steps and participants involved. The average user relies on wallet software and other tools to help construct and execute transactions. There is a risk that the dark pattern-based theories of liability outlined above in the Amazon, TransUnion, and Google enforcement actions may be applied by consumer protection regulators to wallet software or other user interfaces designed to facilitate digital asset transactions.

The primary risk is that consumers using these tools to interact with blockchain networks are manipulated into executing suboptimal transactions. Wallet software and other user interfaces often default users to transactions with preselected conditions. Users may not know that these preselected conditions are not mandatory or that they have the ability to change these conditions. Preselection implicates the default effect cognitive bias – users tend to go with the option that is already chosen for them, even when they can make other choices. Users also may not understand what happens after they sign an instruction using their wallet software to initiate a transaction. As the manner in which users engage with blockchain networks to perform actions evolves, through the use of delegating EOAs to smart contracts or through the use of artificial intelligence agents that are designed to do all of these things for users, the issues around dark patterns will get more complex and it will be even more important to ensure that users understand what is happening and what they are agreeing to when they use these tools.

To protect against these issues and to ensure that consumers have the ability to make meaningful and informed choices about transaction creation and execution, there are a few steps that wallet software providers and hosts of user interfaces might consider implementing.

First, complete and accurate disclosures are critical. These disclosures should be written in plain English and should completely and accurately describe how the relevant software works and how the user will interact with it, and should clearly describe all of the fees and costs associated with transactions that a user can initiate using the software. These disclosures should be easily accessible to the user prior to completing a transaction flow, such as by way of a link to these disclosures in the user interface as opposed to a link at the bottom of the interface in a smaller font.

Second, default settings should be transparent and clearly state that there are default settings that can be changed by users who wish to do so. Ideally, all options would be presented to users with equal prominence so that users' choice is not influenced.

Third, there should be affirmative informed consent and confirmation prior to transaction execution. This will ensure that a user is informed of and agrees to all of the elements of a transaction before signing an instruction.

Fourth, user interface hosts should conduct periodic user interface audits. These audits will help identify friction points in navigation and user experience as well as any potentially unfair or deceptive elements. Such an audit should include:

- a review of user terms for use of plain English, accuracy, and completeness;
- a review of any consent mechanisms, including opt-ins and checkboxes, to confirm they are unambiguous;
- a review of fee disclosures to ensure completeness; and
- an evaluation of features that might have the potential for manipulating consumer behavior, such as features involving gamification.

Conclusion

The enforcement landscape for digital asset activities in the U.S. has changed dramatically in the last year. Despite the pullback in federal enforcement, consumer protection will always be a priority. Both federal and state regulators have broad consumer protection authority that may be applied to digital asset transactions. A recent focus on dark patterns suggests that consumer protection regulators are concerned with these practices. As consumer behavior increasingly shifts towards transacting with digital assets, software providers should be wary of the potential application of dark patterns theories of liability under consumer protection laws and take steps to ensure that when their software is used to enter the dark forest, users understand the risks they are taking.

Endnotes

1 *See, e.g.*, *S.E.C. v. Binance Holdings Ltd.*, 2024 WL 3225974, at *11 (D.D.C. June 28, 2024); *S.E.C. v. Coinbase*, 2024 WL 1304037, at *13, *20; *S.E.C. v. Payward Inc., et al.*, No. 23 Civ. 06003 (WHO), ECF No. 90 (N.D. Cal. Aug. 23, 2024); SEC's Memorandum of Law in Support of Motion for Leave to Amend the Complaint at 24 n.6, *S.E.C. v. Binance Holdings Ltd*, No. 23 Civ. 1599 (D.D.C. Sept. 12, 2024), ECF No. 273-1 ("SEC's Motion for Leave to Amend the Complaint"); Oral Argument, Tr. 21:11, *S.E.C. v. Coinbase*, No. 23 Civ. 4738 (S.D.N.Y. Jan. 17, 2024), ECF No. 101 ("The token itself is not the security."). *Cf. Oregon v. Coinbase*.

2 *See, e.g.*, CFTC Division of Market Oversight and Division of Clearing and Risk, *CFTC-SEC Joint Staff Statement (Project Crypto-Crypto Sprint)* (Sept. 2, 2025); CFTC Division of Market Oversight, *Staff Advisory: Registration Framework for Foreign Boards of Trade (FBOT) Providing Direct Access to Members or Other Participants Located in the United States* (Aug. 28, 2025).

3 *See* Dan Robinson ad Georgios Konstantopoulos, *Ethereum is a Dark Forest* (Aug. 28, 2020), available at: https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest

4 *See generally*, https://ethereum.org/developers/docs/accounts

5 *See* https://eips.ethereum.org/EIPS/eip-7702

6 A function call is the act of executing code or logic defined in a smart contract.

7 Note that wallet software is not required to construct and sign a transaction, but constructing and signing a transaction without wallet software requires technical sophistication and presents security risks that need to be carefully managed.

8 According to certain sources, as of December 2024, upwards of 90% of validators leverage MEV-Boost regularly.

9 FTC Staff Report, *Bringing Dark Patterns to Light* (Sept. 2022), available at: https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

10 *Id.*

11 Amended Complaint, *Federal Trade Commission v. Amazon.com, Inc., et al.*, W.D. Wash., No. 2:23-cv-0932 (Sept. 20, 2023).

12 *See* https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-secures-historic-25-billion-settlement-against-amazon

13 15 U.S.C. § 45(a).

14 15 U.S.C. § 45(n).

15 FTC Policy Statement on Unfairness, Fed. Trade Comm'n (Dec. 17, 1980), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm

16 *Id.*

17 *Id.*

18 *Id.*

19 *Id.*

20 *See* https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf

21 *Id.*

22 *Id.*

23 *Id.*

24 *Id.*

25 *See* 12 U.S.C. § 5481, *et seq.* (2010).

26 *Id.*

27 *Id.*

28 *Id.*

29 *See* https://files.consumerfinance.gov/f/201307_cfpb_bulletin_unfair-deceptive-abusive-practices.pdf

30 *Id.*

31 *Id.*

32 *See* https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-to-address-abusive-conduct-in-consumer-financial-markets

33 *Id.*

34 Complaint, *Consumer Financial Protection Bureau v. TransUnion, et al.*, N.D. Ill., No. 1:22-cv-01880 (April 12, 2022).

35 *Id.*

36 *Id.*

37 *Id.*

38 *Id.*

39 12 U.S.C. § 5552(a)(1).

40 *Id.*

41 *See* https://files.consumerfinance.gov/f/documents/cfpb_strengthening-state-level-consumer-protections_2025-01.pdf

42 *See* https://www.consumerfinance.gov/rules-policy/final-rules/authority-of-states-to-enforce-the-consumer-financial-protection-act-of-2010

43 *See, e.g.*, https://www.attorneygeneral.gov/wp-content/uploads/2022/11/2022-11-14-PA-v.-Google-LLC-AVC-efile.pdf

44 *Id.*

45 *Id.*

46 *Id.*

47 *Id.*

Sarah Chen

Tel: +1 212 701 3759 / Email: swchen@cahill.com

Sarah Chen advises clients on all matters in the space of digital assets and emerging technology, including general corporate, mergers and acquisitions, venture capital investments, securities and financial regulatory matters. Sarah represents a variety of clients in the digital asset space that range from blockchain development companies, foundation entities, digital asset marketplaces and tokenization platforms to venture capital firms, fintech companies and traditional financial institutions. Sarah provides legal advice on securities, commodities and other laws and regulations that may apply to activities involving digital assets and the use of blockchain technology.

Gregory Strong

Tel: +1 302 884 0001 / Email: gstrong@cahill.com

Gregory Strong provides strategic regulatory and litigation advice to clients engaging with blockchain and crypto assets with a focus on securities, commodities, and consumer protection laws and regulations. He has successfully represented clients before the Securities and Exchange Commission (SEC), the Commodities Futures Trading Commission, state securities regulators and various other regulators.

Greg has significant experience successfully engaging with regulators on behalf of clients in the blockchain space with novel legal issues. He was a key member of the team that obtained one of the few no-action letters issued by the SEC with respect to the non-security status of a crypto asset. Greg was also a key member of the team that represented the first successful applicant for a Special Purpose Depository Institution charter before the Wyoming Division of Banking. In addition, he has worked on cutting-edge litigation and transactional matters involving crypto assets.

Frank Weigand

Tel: +1 212 701 3890 / Email: fweigand@cahill.com

Frank J. Weigand is Chair of Cahill's Trading & Markets Group and a member of the firm's Digital Assets and Emerging Technology Group.

Frank focuses his practice on securities, commodities, and digital asset matters, and his clients include a broad range of market participants, including banks, broker-dealers, and funds as well as a full spectrum of participants across the digital asset markets.

Frank advises clients on both regulatory and transactional matters, with a particular focus on solving strategically complex problems and working with clients to develop new products. His many years of experience advising regulated entities in traditional markets gives him the depth and context needed to appropriately advise on regulatory implications relevant to digital asset matters.

From a subject matter standpoint, Frank possesses an intimate knowledge of broker-dealer and securities regulation having previously served as general counsel of two broker-dealers: HSBC Securities (USA) Inc; and Oasis Pro Markets, LLC.

Cahill Gordon & Reindel LLP

32 Old Slip, New York, NY 10005, USA

Tel: +1 212 701 3000 / URL: www.cahill.com

Global Legal Insights – Blockchain & Cryptocurrency Regulation provides in-depth analysis, insight and intelligence across 11 expert analysis chapters and 29 jurisdictions, covering:

- Government attitude and definition
- Cryptocurrency regulation
- Sales regulation
- Taxation
- Money transmission laws and anti-money laundering requirements
- Promotion and testing
- Ownership and licensing requirements
- Mining
- Border restrictions and declaration
- Reporting requirements
- Estate planning and testamentary succession

globallegalinsights.com