



NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION

NASAA's Principles for SEC Crypto-Asset Regulation

Introduction

Fostering innovation and maintaining effective regulation are not only compatible but beneficial and preferred, both for industry and investors. This document offers principles and prescriptions to the Securities and Exchange Commission's Crypto Task Force (the "Task Force") intended to achieve balanced regulatory solutions for issuing and trading crypto-assets¹ that will endure to the same degree as the foundational securities acts themselves.

NASAA regards the Commission's effort to understand and determine how to regulate crypto-assets as an opportunity for regulators to learn how to respond both nimbly and responsibly to technological innovations. As the advent of distributed ledger technology has shown, major innovations can happen unexpectedly. Further, given the rapid development of predictive analytics and artificial intelligence, it is a given that paradigm-shifting technological innovations are just over the horizon. How well regulators meet today's challenges will set the stage for our ability to adapt to future innovations while preserving the ability to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation.

General Principles

NASAA asks the Task Force to keep the following principles in mind when it forms its recommendations in order to achieve a stable evolution of regulation that embraces crypto-assets while preserving the essential features of effective regulation:

- **Investor protection** must be the central part of any proposed regulation.
- **Robust disclosures** must be simple enough for novice investors to understand the risks of buying and trading crypto-assets and should be available on a trusted site administered by a regulator.
- **Exemptive frameworks** for crypto-assets and businesses are better than jurisdictional exclusions because they can be tailored and adjusted as circumstances change.
- **State antifraud and examination authorities** must be preserved.

¹ While various terms have been used to describe assets that rely on distributed ledger technology, this document uses "crypto assets" to accord with current SEC practice.

Specific Recommendations

These recommendations apply the principles above to certain questions in Commissioner Peirce’s statement “There Must Be Some Way Out of Here” (the “RFI”).²

I. Investor Protection

Unfortunately, the world of crypto-assets has been rife with fraud.³ This is due in part to features of distributed ledger technology that can facilitate bad actors, particularly the pseudonymous nature of crypto-assets, their vulnerability to theft from hacking, and the irreversibility of blockchain transactions. The Task Force should account for these features and vulnerabilities when forming recommendations.⁴

A. Trading

The RFI asks if “open-source data [is] sufficient for the market to monitor trading and therefore what non-public information might warrant mandatory disclosure?”⁵ The answer to the first part of the question is “no;” open-source data may be able to indicate improper trading, but it will not show who is involved.⁶ Crypto-asset intermediaries should therefore be required to follow

² SEC Commissioner Hester M. Peirce, *There Must Be Some Way Out of Here* (Feb. 21, 2025), <https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125>.

³ Just a few examples include online relationship scams (sometimes referred to as “pig butchering”), market manipulation, and pump-and-dump schemes. See Dylan Butts, *Crypto scams likely hit a new record in 2024, driven by ‘pig butchering’ and AI, says Chainalysis*, CNBC (Feb. 13, 2025, 11:08 PM), <https://www.cnbc.com/2025/02/13/crypto-scams-thrive-in-2024-on-back-of-pig-butchering-and-ai-report.html>; Chainalysis, *Market Manipulation: Suspected Wash Trading on Select Blockchains May Account for Up To \$2.57 Billion in Trading Volume* (Jan. 29, 2025), <https://www.chainalysis.com/blog/crypto-market-manipulation-wash-trading-pump-and-dump-2025/>; JT Hamrick et al., *An examination of the cryptocurrency pump and dump ecosystem* (last revised Jan. 9, 2021), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3763113_code1489.pdf?abstractid=3303365&mirid=1.

⁴ President Trump has directed the SEC and other Working Group agencies to propose a federal regulatory framework governing the issuance and operation of digital assets that considers “consumer protection” among other factors. Exec. Order No. 14178, *Strengthening American Leadership in Digital Financial Technology* (Jan. 23, 2025), <https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/>.

⁵ RFI, Question 18.

⁶ The Commission has previously recognized that the ability to identify manipulative bitcoin spot trading in a manner that satisfies Section 6(b)(5) of the Securities Exchange Act of 1934 can be accomplished by relying on the Chicago Mercantile Exchange’s (“CME”) futures surveillance capabilities. See Order Granting Accelerated Approval of Proposed Rule Changes, as Modified by Amendments Thereto, to List and Trade Bitcoin-Based Commodity-Based Trust Shares and Trust Units, SEC Rel. No. 34-99306 (Jan. 10, 2024), <https://www.sec.gov/files/rules/sro/nysearca/2024/34-99306.pdf>. The order recognized that there is no equivalent spot surveillance mechanism, and the Commission has previously rejected attempts to satisfy the requirements of Section 6(b)(5) by relying on the perceived liquidity of crypto-asset spot markets. See, e.g., Order Setting Aside Action by Delegated Authority and Disapproving a Proposed Rule Change, as Modified by Amendments No. 1 and 2, to List and Trade Shares of the Winklevoss Bitcoin Trust, SEC Rel. No. 34-83723 (Jul. 26, 2018), <https://www.sec.gov/files/rules/other/2018/34-83723.pdf>. Importantly, it should be noted that CME surveillance can

know your customer requirements in order to be able to answer regulator inquiries about potentially improper trading. Indeed, regulators need to have the same powers to monitor and examine crypto-asset intermediaries as currently exist for securities market intermediaries. Further, trading platforms should be required to develop written policies and procedures to ensure that trades are legitimately authorized by customers.

B. Custody

The RFI asks whether the Commission should “amend existing rules, propose new rules, or provide guidance to facilitate custody arrangements for crypto assets.”⁷ In general, custody requirements should apply any time a customer gives an asset to an intermediary, and any new or amended rules should fully serve the purposes of existing custody requirements; namely, to protect customer assets from misuse, loss, theft, conflicts of interest, or the failure of the registrant holding them.

NASAA understands that crypto-asset wallets and encryption keys present unique handling challenges but nevertheless maintains that the amount of accommodation necessary should be determined by the technological limitations of distributed ledger technology, and not by the preferences of current crypto-businesses. For example, while some trading platforms may prefer to hold all customer assets in a vertical stack arrangement to facilitate trading, trading platform regulatory models that incorporate third party custody safeguards already exist.⁸ If for no other reason, separate custody of crypto-assets protects customers from losing their assets if the trading platform becomes insolvent.⁹ Separate custody could also have prevented outright frauds like FTX.

Further, there is nothing inherent in distributed ledger technology that prevents the use of current custody safeguards, including rigorous written policies and procedures, periodic and surprise audits, a robust examination schedule, and recordkeeping requirements that account for the full transactional life of crypto-assets taken from customers, held off-chain, and traded in an

identify specific exchange members engaged in potential misconduct. Blockchain analysis alone cannot and is therefore an inadequate means to monitor for misconduct.

⁷ RFI, Question 21.

⁸ See *Coinbase Canada Inc. (Re)* (2024), 47 O.S.C. Bull. 3081, paras. 95-109 (Can. Ont. Sec. Com.), https://www.osc.ca/sites/default/files/2024-04/20240411_osc_b_2715.pdf (requiring trading platform to custody not less than eighty percent of crypto-assets in segregated accounts with Acceptable Third-party custodians, which in this application was an affiliated entity of the platform); *NDAX Canada Inc. (Re)* (2025), 48 O.S.C. Bull. 159, para. 75 (Can. Alta. Sec. Com.), https://www.osc.ca/sites/default/files/2025-01/ord_20241219_ndax-canada-inc_0.pdf (requiring trading platform to custody not less than eighty percent of crypto-assets in segregated accounts with Acceptable Third-party Custodians, which in this application were affiliated and non-affiliated custodians regulated as trust companies). In its letter to the Task Force, Coinbase acknowledged that offsite custody would be acceptable. Letter from Paul Grewal, Chief Legal Officer, Coinbase Global, Inc., to Commissioner Hester M. Peirce, Chair, SEC Crypto Task Force, at 16 (Mar. 19, 2025), <https://www.sec.gov/files/ctf-input-grewal-2025-3-19.pdf>.

⁹ See Jonathan Weil, *A Lingering Question at Coinbase: Who Really Owns the Customers' Crypto?*, WALL ST. J. (Feb. 19, 2025, 5:30 AM), <https://www.wsj.com/finance/currencies/coinbase-crypto-ownership-accounting-7c97b26a> (stating that if Coinbase went bankrupt, customer tokens could be considered part of the bankruptcy estate, leaving customers to be treated as unsecured creditors).

omnibus fashion.¹⁰ Distributed ledger technology can help with some of these recordkeeping and examination requirements, but it is not in and of itself a substitute for tailored custody requirements based on proven regulatory premises.

C. *Cybersecurity*

While the RFI does not mention cybersecurity, it is critically important to the handling and safekeeping of crypto-assets. Because crypto-asset trading platforms handle customer assets online, the Task Force should pay special attention to cybersecurity requirements. U.S. exchanges are subject to Regulation SCI, which requires them to maintain strict cyber hygiene standards, report cybersecurity failures and breaches to affected persons and the Commission, take immediate corrective actions, review their systems annually, make periodic reports to the Commission, and coordinate business continuity and disaster recovery activities with other SCI entities.¹¹ The Commission established these requirements because exchanges are essential to market functioning and their failure could have systemic consequences.

If anything, the cybersecurity needs of trading platforms are even more critical. Trading platforms have repeatedly fallen victim to hacking,¹² and crypto-assets are particularly attractive to thieves because the irreversibility of blockchain trades means they are largely unrecoverable once stolen. NASAA believes trading platforms should meet standards at least as rigorous as those applied to exchanges, and the Task Force should recommend cybersecurity rules for all crypto-intermediaries as rigorous as necessary to reasonably ensure the protection of customer assets.¹³

¹⁰ At least one other commenter agrees. See Letter from Scott Walker et al., Chief Compliance Officer, A.H. Capital Management, LLC, to Commissioner Hester M. Peirce, Chair, SEC Crypto Task Force, at 8 (Apr. 9, 2025), <https://www.sec.gov/files/ctf-input-horowitz-040925.pdf> (stating that “[w]e strongly support requiring crypto custodians to undergo an annual surprise audit by a PCAOB-registered auditor.”).

¹¹ 17 C.F.R. §§ 242.1000-07 (2025).

¹² See, e.g., REUTERS, *Coinbase warns of up to \$400 million hit from cyberattack*, (May 15, 2025 6:59 PM), <https://www.reuters.com/business/coinbase-says-cyber-criminals-stole-account-data-some-customers-2025-05-15/>; REUTERS, *Bybit says \$1.5 billion worth of crypto stolen in ether wallet hack*, <https://www.reuters.com/technology/crypto-exchange-bybit-says-ether-wallet-hacked-2025-02-21/> (last updated Feb. 21, 2025, 7:24 PM); *Russian Nationals Charged With Hacking One Cryptocurrency Exchange and Illicitly Operating Another*, U.S. DEP’T OF JUST. (Feb. 6, 2025), <https://www.justice.gov/archives/opa/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating-another>; David Uberti, *How Hackers Target Bridges Between Blockchains for Crypto Heists*, WALL ST. J. (Apr. 5, 2022, 5:30 AM), <https://www.wsj.com/articles/how-hackers-target-bridges-between-blockchains-for-crypto-heists-11649151001>; Tom Wilson & Pushkala Aripaka, *Jump Trading replaces stolen Wormhole funds after \$320 mln crypto hack*, REUTERS, <https://www.reuters.com/technology/crypto-network-wormhole-hit-with-possible-320-mln-hack-2022-02-03/> (last updated Feb. 3, 2022, 5:20 PM); Gertrude Chavez-Dreyfuss & Michelle Price, *How hackers stole \$613 million in crypto tokens from Poly Network*, REUTERS, <https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/> (last updated Aug. 12, 2021, 11:17 PM); Takashi Mochizuki & Paul Vigna, *Cryptocurrency Worth \$530 Million Missing From Japanese Exchange*, WALL ST. J., <https://www.wsj.com/articles/cryptocurrency-worth-530-million-missing-from-japanese-exchange-1516988190> (last updated Jan. 26, 2018, 4:48 PM).

¹³ See Regulation S-P, Rule 30(a), 17 C.F.R. § 248.30(a) (2025) (mandating that all covered institutions must develop, implement and maintain written policies and procedures “reasonably designed to [e]nsure the security and confidentiality of customer information; [p]rotect against any anticipated threats or hazards to the security or integrity of customer information; and [p]rotect against unauthorized access to or use of customer information that

II. Robust, Simple Disclosures

A. *Issuer and Product Disclosures*

Most observers and the courts agree that primary offerings, where a crypto-asset is combined with an issuer’s promise to build or promote a business, falls within the definition of an “investment contract” articulated in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). The debate begins when there is an arguable separation between secondary trading motivations and an issuer’s efforts or continued existence.

It is doubtful that clean lines can be drawn here because there is a wide spectrum of promotional efforts and levels of control that can play into the question of whether continuing disclosure is needed about a crypto-asset issuer. Also, it is not certain that crypto-assets can be neatly divided between securities and commodities by measuring decentralization or the maturity of a blockchain. Some commentators have cast doubt on the viability of such measures,¹⁴ and others reject the concept outright.¹⁵ However, NASAA also recognizes that commenters are attempting to classify crypto-assets into categories that may matter to crypto-asset purchasers

could result in substantial harm or inconvenience to any customer.”). The Commission might also want to explore borrowing from well-regarded state models. See Cheryl Winokur Munk, *Six Ways to Lose All Your Crypto*, WALL ST. J. (Mar. 19, 2025, 11:00 AM), <https://www.wsj.com/tech/cybersecurity/cryptocurrency-safety-scams-what-to-know-0d85877e> (quoting Howard Greenberg, president of the American Blockchain and Cryptocurrency Association, who states that “[i]nvestors should buy cryptocurrency through an exchange that’s registered with the New York State Department of Financial Services, because of the agency’s stringent reporting requirements and rules . . . [i]f you pick [an exchange] that’s approved there, that would be, to me, the closest to a gold standard that’s available.”).

¹⁴ Angela Walch, *Deconstructing ‘Decentralization’: Exploring the Core Claim of Crypto Systems*, in *Crypto Assets: Legal and Monetary Perspectives* 39, 60 (Chris Brummer ed., Oxford Univ. Press 2019), also available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326244 (in the context of an explanation of the difficulties of assessing decentralization, stating that “[t]he decentralization of a given blockchain system is such a complex, undefined concept that it is a bad idea to use it to make legal decisions at this point in time.”); Lee Reiners, *Prepared Statement for SEC’s Crypto Task Force March 21, 2025 Roundtable titled “How We Got Here and How We Get Out – Defining Security Status” and Responses to “Security Status” Questions in SEC Commissioner Hester Peirce’s February 21, 2025 Statement Titled “There Must Be Some Way Out of Here,”* at 29 (Mar. 21, 2025), <https://www.sec.gov/files/ctf-input-reiners-2025-3-18.pdf> (observing that “decentralization exists along a spectrum across multiple dimensions (governance, asset, user, application, data, network, protocol, hardware)” and that “[d]etermining when these dimensions are decentralized enough to ensure profits don’t come from others’ efforts is futile.”).

¹⁵ Hilary J. Allen, *The Superficial Allure of Crypto*, INT’L MONETARY FUND (Sept. 2022), <https://www.imf.org/en/Publications/fandd/issues/2022/09/Point-of-View-the-superficial-allure-of-crypto-Hilary-Allen> (stating that “unfortunately, crypto does not live up to its claims of decentralization”); Sirio Aramonte et al., *DeFi risks and the decentralisation illusion*, BIS (Dec. 6, 2021), https://www.bis.org/publ/qtrpdf/r_qt2112b.htm (stating that “[t]here is a ‘decentralisation illusion’ in DeFi since the need for governance makes some level of centralisation inevitable and structural aspects of the system lead to a concentration of power.”); Letter from Stuart Alderoty et al., Chief Legal Officer, Ripple Labs, Inc., to Commissioner Hester M. Peirce, Chair, SEC Crypto Task Force, at 3, 7 (Mar 21, 2025), <https://www.sec.gov/files/ctf-input-ripple-2025-3-21.pdf> (observing that decentralization is “a concept found nowhere in the law” and asserting that “there are provisions within the latest proposal that do not advance the goals of the Commission, such as equating ownership of tokens with control on a network or that meeting a certain ownership percentage tips the scale one way or the other on control of a network.”).

separately from issuer promotional efforts.¹⁶

The Crypto Task Force should, therefore, recommend rulemaking that would result in the development of two forms of disclosure for crypto-asset offerings. The first should be disclosures by crypto-asset issuers about such things as the nature of the issuing business, the use of proceeds, the business's principals and material affiliates, and other information typically considered by a reasonable investor as material to the decision to purchase a crypto-asset.¹⁷

The second should be disclosures about the crypto-assets themselves and their underlying networks, which would be relevant regardless of whether the crypto-assets are characterized as securities or commodities, such as uses, governance, and technological features that would be material to understanding any enduring value the asset may have apart from the existence of the issuer.

NASAA also believes both forms of disclosure should be filed with the Commission on the Electronic Data Gathering, Analysis, and Retrieval ("EDGAR") system and notice filed with state securities regulators.¹⁸ Having a single place to find information about crypto-asset issuers and their tokens is preferable to an approach that leaves investors on their own to find and judge the reliability of information on random web pages. At the same time, the Commodity Futures Trading Commission ("CFTC") has no equivalent filing system, and it makes no sense to ask the CFTC to build one. Further, the anticipated regulatory trajectory for crypto-asset issuances is, if anything, from classification as a security to a commodity, and so EDGAR is a good place to record the history of the business and the asset.

Disclosures of both kinds described above would be helpful not only to investors, but also intermediaries. For instance, broker-dealers are required to understand the products they recommend to customers,¹⁹ and investment advisers need to have the same level of understanding to meet their fiduciary duties to clients.²⁰ Therefore, requiring centralized product disclosures

¹⁶ See, e.g., *Proposed Information Guidelines for Certain Tokens Made Available in the United States*, GLOB. DIGIT. ASSET & CRYPTOCURRENCY ASS'N. (Oct. 20, 2024), <https://global-dca.org/wp-content/uploads/2025/01/Information-Guidelines-for-Tokens-Available-in-US-FINAL-Jan-31-2025.pdf>; Teresa Goody Guillén & Isabelle Corbett Sterling, *Paving the Path for Crypto Clarity: A Framework for Digital Asset Regulatory Structure* (discussion draft Feb. 17, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5156725 (cited with permission).

¹⁷ Because many crypto-businesses appear to aspire to raise money, build functionalities and then disappear, NASAA also believes that certain essential issuer disclosures should be required regardless of whether an issuance is made on a registered or exempt basis.

¹⁸ NASAA's Electronic Filing Depository ("NASAA EFD") can facilitate this process because it is set up to consume data from EDGAR. See NASAA EFD, Version 1.2.1, <http://www.nasaaefd.org>.

¹⁹ 17 C.F.R. § 240.151-1(a)(2)(ii)(A) (2025) (requires broker-dealers and their associated persons to "[u]nderstand the potential risks, rewards, and costs associated with the recommendation . . .").

²⁰ See, e.g., Commission Interpretation Regarding Standard of Conduct for Investment Advisers, SEC Rel. No. IA-5248, at 17 (July 12, 2019), <https://www.sec.gov/files/rules/interp/2019/ia-5248.pdf> (explaining that "an investment product's or strategy's investment objectives, characteristics (including any special or unusual features), liquidity, risks and potential benefits, volatility, likely performance in a variety of market and economic conditions, time horizon, and cost of exit" are important "to consider when determining whether a security or investment strategy involving a security or securities is in the best interest of the client.").

would benefit all market participants.

B. Registration Safe Harbors

The RFI asks whether the Commission should create a safe harbor for crypto-asset issuances.²¹ NASAA does not believe such an approach is necessary because crypto-asset issuers have already proven that they can make offerings within current registration and exemptive frameworks.²² The Commission’s Division of Corporation has also recently released disclosure guidance for registered crypto-asset securities offerings.²³ Further, at least one notable Task Force commenter, an expert on capital formation, has asserted that current exemptions are adequate.²⁴ Taken together, it is clear that no new exemption or accommodation needs to be created.

Given all of this, the question should be what distinguishes the few issuers who have used current frameworks from the majority that have not? It is not that distributed ledger technology makes compliant issuances impossible. Instead, it is more likely some combination of the ill-fitting nature of some disclosure requirements and the current business preferences of crypto-asset issuers. While accommodations for the first circumstance (“ill-fitting disclosure requirements”) may warrant the development of tailored disclosures to address the unique features of distributed ledger technology, accommodations simply to meet current preferences is not.

III. Exemptive Frameworks

A. Issuer Relief

With respect to the taxonomy of digital assets, the RFI seeks comment on “creative solutions that comport with the Commission’s statutory framework.”²⁵ They already exist; Section 28 of the Securities Act of 1933 (the “Securities Act”) and Section 36 of the Securities Exchange Act of 1934 (the “Exchange Act”) allow the Commission to “conditionally or unconditionally exempt any person, security, or transaction, or any class or classes of persons, securities, or transactions” from the provisions of both acts or their underlying rules or regulations “to the extent that such exemption is necessary or appropriate in the public interest, and is consistent with the

²¹ RFI, Questions 10-14.

²² *See, e.g.*, Open Props Inc. (formerly YouNow), <https://www.sec.gov/edgar/browse/?CIK=1725129>; Hiro Systems PBC (formerly Blockstack), <https://www.sec.gov/edgar/browse/?CIK=1693656>; CERES Coin LLC, <https://www.sec.gov/edgar/browse/?CIK=1734118> (all examples of exempt offerings). Crypto-asset issuers have also offered registered securities. *See, e.g.*, INX Ltd., <https://www.sec.gov/edgar/browse/?CIK=1725882>.

²³ Div. of Corp. Fin., Statement on Offerings and Registrations of Securities in the Crypto-Asset Markets, SEC (Apr. 10, 2025), https://www.sec.gov/newsroom/speeches-statements/cf-crypto-securities-041025#_ftnref3.

²⁴ Letter from Sara Hanks, Founding Partner, CrowdCheck Law LLP, to Commissioner Hester M. Pierce and Members of the SEC Crypto Task Force, at 2, 3 (Mar. 19, 2025), <https://www.sec.gov/files/ctf-input-hanks-2025-3-19.pdf> (stating that “[w]e believe that Regulation A currently provides the most appropriate option for public offerings of either tokenized traditional securities or novel crypto assets, without violence to the original objectives of Regulation A or the need for significant rulemaking” and that “[w]e believe that if an exemption under Regulation A is available, there would be no need for a safe harbor of the kind described.”).

²⁵ RFI.

protection of investors.” To the extent the Task Force determines there is a need for the Commission to give clarity to crypto-asset issuers with respect to their registration obligations, it should recommend exemptive relief, either for certain instruments wholesale (in the vein of Securities Act Section 3) or for specific transactions (in the vein of Securities Act Section 4).

As a general matter, an exemptive approach is preferable to excluding broad categories of tokens from the securities laws and is regulatorily sound in part because the delineation between securities and commodities is not clear, and in fact may become more muddled in practice as the Commission seeks to apply Task Force ideas to real world assets and transactions. On March 21, 2025, the Commission held the first roundtable in its “Spring Sprint Toward Crypto Clarity” entitled “How We Got Here and How We Get Out – Defining Security Status.”²⁶ One clear result from that discussion was that a panel of some of the most experienced and thoughtful persons in the crypto-asset space could not agree on the extent to which crypto-asset transactions fall within the securities laws. This discussion largely mirrored the debate that had been playing out in the courts prior to the current administration.²⁷ Consensus was lacking then and, despite the Task Force’s earnest efforts, clarity is still lacking on this question. Further, to the extent that legislation will need implementing regulations, confusion and disagreement about this question will persist.

The Task Force should therefore recommend an exemptive approach because doing so would allow the Commission to provide regulatory certainty in a manner that is relatively quick, can be tailored and limited to the types of crypto-assets being developed and offered, and can be adjusted in light of emerging circumstances. As we noted at the outset of our submission, new innovations are certain and may happen unexpectedly and quickly. The Commission should build nimbleness into its regulatory quiver by using its present tools in a thoughtful and flexible manner. NASAA also prefers exemptive solutions because the Commission would be required to undertake an analysis and create a record as to why the proposed exemptive relief is in the public interest and consistent with the protection of investors. That record could then serve as the criteria against which exemptions could be measured and, if necessary, adjusted or rolled back.

In short, exemptive relief coupled with meaningful disclosure and investor protection is a good way to (i) provide further clarity, (ii) meet innovation with flexibility, and (iii) sustain trust.

B. Antifraud Concerns

From NASAA’s perspective, perhaps the most important benefit of pursuing an exemptive framework is that doing so would preserve the antifraud jurisdiction of both the Commission and state securities regulators. The Commission has maintained that pursuing fraud – particularly

²⁶ SEC, *Crypto Task Force 01*, YOUTUBE (Mar. 21, 2025), <https://www.youtube.com/watch?v=o22EH9Hr6DA>; SEC, *Crypto Task Force 02*, YOUTUBE (Mar. 21, 2025), https://www.youtube.com/watch?v=T_HEoRPS4N8.

²⁷ See *SEC v. Ripple Labs, Inc.*, 682 F. Supp. 3d 308, 328 (S.D.N.Y. 2023); *SEC v. Terraform Labs Pte. Ltd.*, 684 F. Supp. 3d 170, 184 (S.D.N.Y. 2023); *SEC v. Coinbase, Inc.*, 726 F. Supp. 3d 260 (S.D.N.Y. 2024) (finding that the SEC sufficiently alleged that defendant offered and sold its Staking Program as an investment contract).

violative conduct aimed at retail investors – remains essential to its efforts.²⁸ NASAA is reassured by the Commission’s continued commitment to fight fraud because, as is explained in more detail below, crypto-asset-related fraud has become a leading threat to retail investors, and particularly to older investors. State securities regulators must retain examination and antifraud authority to protect our citizens and sustain trust in regulated markets, and we need Commission enforcement staff to be on the front lines with us.

C. *Intermediary Relief*

Another benefit of tailoring exemptions or offering registrations is that doing so would keep in place rules related to how broker-dealers and investment advisers run their businesses, and the standards of conduct to which they are expected to adhere. In other words, through exemptive relief, the Commission can maintain, and does not have to revisit, large portions of the federal securities laws while giving relief around securities registration issues.

The RFI asks whether the Commission should “create a new entity registration status with tailored registration requirements for any platform that trades crypto assets that are securities.”²⁹ In general, it is NASAA’s view that crypto-asset intermediaries should be required to adhere to current requirements of intermediaries that are designed to ensure resiliency and investor protection. Examples include business conduct rules, net capital and liquidity requirements, data protection requirements, custody requirements as previously discussed, and licensing and qualification requirements for both firms and associated persons.

More specifically, there are already registration categories for whatever form crypto-asset trading might take, whether it be centrally-cleared exchanges, bilateral inter-dealer quotation systems (such as OTC Markets) or wholly internal alternative trading systems. So long as one of these models can be adapted to address the trading of crypto-asset securities, it makes little sense to expend limited Commission resources to formulate a new rule set with related forms and processes for a new form of registrant.³⁰ Instead, modifying existing registration categories is more regulatorily efficient and gives existing registrants the same chance to trade crypto-asset securities as would be provided to new, dedicated crypto-asset businesses.³¹

²⁸ REUTERS, *SEC to focus on traditional cases under new leadership, acting director says*, <https://www.reuters.com/world/us/sec-focus-traditional-cases-under-new-leadership-acting-director-says-2025-03-24/> (last updated Mar. 24, 2025, 6:23 PM).

²⁹ RFI, Question 15.

³⁰ NASAA notes its view is shared by other commenters. *See* SIFMA, *SEC Crypto Task Force: Initial Feedback*, at 3 (Mar. 2025), <https://www.sec.gov/files/ctf-memo-sifma-2025-3-14.pdf> (stating that “[t]o the extent possible, policymakers should apply existing and well-understood regulatory frameworks to digital assets rather than creating entirely new regulatory architectures.”); Grewal Letter, *supra* note 8, at 15 (stating that “[w]ith minimal exemptive or no-action relief, Regulation ATS can be used to facilitate trading of digital securities on centralized trading platforms”); Letter from Daniel M. Gallagher, Chief Legal, Compliance and Corporate Affairs Officer, Robinhood Markets, Inc., to SEC Acting Chairman Mark Uyeda and Commissioner Hester M. Peirce, at 4-5 (Mar. 13, 2025), <https://www.sec.gov/files/ctf-input-robinhood-2025-03-13.pdf> (stating that existing exemptive relief powers can address registration requirements, books and records requirements, antifraud protections, custody requirements, and transaction reporting obligations).

³¹ *See* Letter from John A. Zecca, Executive Vice President, Global Chief Legal, Risk & Regulatory Officer,

An exemptive relief approach would help limit regulatory relief to the degree necessary to address the technological limits of distributed ledger technology while preserving most of the good works and hard-earned lessons built into the federal securities laws. Other commentators agree.³²

IV. Preserving State Authorities

As NASAA’s 2024 Enforcement Report and recent Top Investor Threats Survey make clear, crypto-facilitated frauds are among the leading threats to retail investors.³³ In 2023, crypto-assets other than NFTs and staking were involved in 50% more state enforcement actions than the next most common product.³⁴ The number of these cases has increased steadily since 2020, and it coincides with the increasing use of the internet and social media to market questionable investments and perpetrate fraud.³⁵ Although legitimate financial services firms are using these platforms to advertise new products and engage with clientele, bad actors are also using social media to more effectively recruit victims and defraud the public.³⁶ Moreover, these trends appear to correlate with the day-to-day experience of state and federal regulators, who are frequently inundated with referrals, complaints, reports, and enforcement matters involving pig butchering and other similar scams.³⁷ State regulators have led the way in pursuing crypto frauds and have

Nasdaq, Inc., to SEC Crypto Task Force, at 2 (Feb. 12, 2025), <https://www.sec.gov/files/nasdaq-020625.pdf> (stating that “if any venue is to trade both digital assets securities and non-securities digital assets, all venues should be permitted to do so, including national securities exchanges.”).

³² See Letter from Tyler Gellasch, President and CEO, Healthy Markets Association, to Commissioner Hester M. Peirce, Chair, SEC Crypto Task Force, at 2 (Apr. 11, 2025), <https://www.sec.gov/files/ctf-input-gellasch-hma-041125.pdf> (stating that “the SEC should start with [existing] rules as the base text, and then tweak them to address the unique nature of digital assets . . .”).

³³ *NASAA Highlights Top Investor Threats for 2025*, NASAA (Mar. 6, 2025), <https://www.nasaa.org/75001/nasaa-highlights-top-investor-threats-for-2025/#:~:text=This%20year%2C%20the%20most%20critical,the%20United%20States%20and%20Canada;NASAA%20Enforcement%20Report%20and%20Top%20Threats%20for%202024>, NASAA, at 4-6, 11-14 (Oct. 22, 2024), https://www.nasaa.org/wp-content/uploads/2024/10/FINAL_2024-Enforcement-Report.pdf.

³⁴ *NASAA Enforcement Report*, *supra* note 33, at 5-6. NASAA has not yet collected data for enforcement actions taken in 2024.

³⁵ *See id.* at 11 (data reflecting 19% increase in investigations and 12% increase in enforcement actions involving the use of the internet and social media); *see id.* at 13 (Table: Digital Asset Enforcement Trends showing year-over-year increases in crypto-asset investigations and enforcement actions).

³⁶ *See* NASAA, *NASAA Releases 2024 Enforcement Report* (Oct. 22, 2024), <https://www.nasaa.org/73977/nasaa-releases-2024-enforcement-report?qoid=current-headlines> (“Fraudsters often exploit the buzz that comes with innovation and technology to take advantage of investors. Combine that with the many ways in which technology and social media link us together and bad actors find significant opportunities to try and rip off investors.”).

³⁷ For example, the California Department of Financial Protection and Innovation publishes a “Crypto Scam Tracker” based on complaints made to the agency. Based on the available data, more than 60% of the entries involve pig butchering. Cal. Dep’t of Fin. Prot. and Innovation, *Crypto Scam Tracker*, <https://dfpi.ca.gov/consumers/crypto/crypto-scam-tracker/> (last updated Apr. 30, 2025, 6:15 PM) (search for “pig butchering” yields 228 entries, filtered from 357 total entries).

been able to disrupt fraudulent activity and return millions of dollars to retail investors.³⁸ Given the prevalence of crypto-asset-related fraudulent activities, states are particularly concerned about being deprived of the ability to protect their citizens from this prevailing threat. To inhibit state regulators through jurisdictional exclusion – rather than exemptions – would leave retail investors in the cold, not only from regulatory violations, but from outright fraud.³⁹ There is no sensible policy reason to do so.

V. Conclusion

NASAA thanks the Task Force for its extensive and thoughtful work, and for the courtesy it has extended to NASAA and others to have our views heard. Reaching sound and lasting answers to the challenges presented by crypto-assets will not be easy. However, so long as the Task Force maintains a focus on solutions that protect investors, including robust disclosures and the preservation of antifraud authorities, it can pursue innovation in a way that is safe and confidence-boosting for investors and the markets.

³⁸ See, e.g., Tex. State Sec. Bd., *Commissioner Files Action Against Alleged Former GS Partners Agents – Parties Accused of Promoting New Crypto Scheme Issued by Trage Technologies* (Oct. 10, 2024), <https://ssb.texas.gov/news-publications/commissioner-files-action-against-alleged-former-gs-partners-agents-parties> (discussing alleged fraudulent crypto-asset arbitrage investment purporting to be registered with the SEC); K100 4REAL LTD d/b/a K-100 et al., *Desist and Refrain Order*, Cal. Dep’t of Fin. Prot. and Innovation (Aug. 20, 2024), <https://dfpi.ca.gov/wp-content/uploads/sites/337/2024/08/D-R-K100-4Real-LTD.pdf> (alleging fraud involving online crypto-asset trading platform); N.Y. State Att’y Gen., *Attorney General James Sues Cryptocurrency Companies NovaTechFx and AWS Mining for Defrauding Investors of More than \$1 Billion* (June 6, 2024), <https://ag.ny.gov/press-release/2024/attorney-general-james-sues-cryptocurrency-companies-novatechfx-and-aws-mining> (detailing charges involving illegal crypto-asset pyramid scheme targeting Haitian New Yorkers). In addition to efforts by state regulators, the British Columbia Securities Commission recently led a coordinated operation by securities regulators, police agencies, crypto-asset trading platforms, and a blockchain analysis firm to disrupt fraudulent schemes by identifying and warning owners of compromised Ethereum wallets. B.C. Sec. Comm’n, *BCSC disruption of overseas crypto fraud alerts nearly 100 Canadian victims* (Apr. 16, 2025, 17:01 ET), <https://www.newswire.ca/news-releases/bcsc-disruption-of-overseas-crypto-fraud-alerts-nearly-100-canadian-victims-889820673.html#:~:text=Note:%20Video%20and%20photos%20from.steps%20to%20prevent%20further%20losses>

³⁹ For this reason, the federal securities laws clarify the retention of state antifraud and examination authorities. See 15 U.S.C. §§ 77p(e) and 78bb(f)(4) (Securities Act and Exchange Act provisions preserving state jurisdiction to investigate and bring enforcement actions); and 15 U.S.C. § 78bb(i)(2)(B) (Exchange Act provision preserving state jurisdiction to examine funding portals and bring enforcement actions for violations of state law).