March 30, 2026

By electronic submission

The Honorable Hester M. Peirce and Members of the Crypto Task Force
U.S. Securities and Exchange Commission
100 F Street NE Washington, DC 20549-0213

Re: Automated Market Makers and the Consistent Application of Securities Market Regulations

Commissioner Peirce and the Crypto Task Force:

The Securities Industry and Financial Markets Association[1] ("SIFMA") appreciates the opportunity to submit this letter to the Crypto Task Force to highlight key considerations related to the use of automated market makers ("AMMs") in the trading of tokenized securities and the importance of applying longstanding securities market safeguards in a technology-neutral manner.

Executive Summary

Automated Market Makers ("AMMs") are blockchain-based trading mechanisms that use pooled liquidity and algorithmic pricing formulas, rather than traditional order books, to intermediate asset trades in decentralized finance ("DeFi") markets. AMM platforms have experienced significant growth in trading volumes[2]—underscoring their increasing relevance to the digital asset ecosystem. As the Commission evaluates whether and how AMMs may support trading in tokenized securities, the central policy question is not whether AMMs are "decentralized," but whether the functions they perform align with activities already regulated under the federal securities laws.

SIFMA believes the Commission should maintain technology neutrality by regulating AMMs based on their market function rather than protocol architecture. "Decentralized" execution often shifts—

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

[2] For example, Uniswap v4 has processed over $350 billion in volume. See https://dexanalytics.org/metrics/v4

rather than eliminates—core intermediary functions such as order routing, execution, pricing, and custody transfer. Where those functions are present, the corresponding regulatory obligations should apply.

- AMMs as observed in the unregulated crypto markets have many features which are distinctly different from market infrastructure seen in established, regulated securities markets. These features result in weakened investor protections and increased risks to market integrity.
- Some of these features represent design choices by AMM operators, such as price slippage, conflicts of interest for liquidity providers, pseudonymous open trading, lack of market manipulation controls and unclear governance. Others are intrinsic to AMMs, such as lack of dispute resolution and liquidity issues. Any application of AMMs to the trading of tokenized securities would need to address these concerns.
- Regulation of AMM-driven markets for tokenized securities should distinguish between the AMM itself (code which operates a trading model), the organizations which develop markets based on that code (such as foundations and decentralized autonomous organizations (DAOs)), applications used to interface with those platforms (*e.g.* front ends), and the roles market participants play in supporting AMM-driven markets (*e.g.* liquidity providers).
- It is critical to consistently apply regulatory requirements to entities whose roles in AMM-driven tokenized securities markets are substantively like exchanges, brokers, market makers, or other regulated functions. While there is a diversity of AMM models, it is possible to clearly identify combinations of services and responsibilities which clearly align with established regulatory roles.

Integrating AMM-based models into securities markets without addressing these gaps would represent a departure from, rather than an evolution of, the investor protection and market integrity standards embedded in U.S. equity market structure.

Introduction

Automated Market Makers (“AMMs”) are blockchain-based trading mechanisms that use pooled liquidity and algorithmic pricing formulas, rather than traditional order books, to intermediate asset trades in decentralized finance (“DeFi”) markets. In an AMM, users called liquidity providers (“LPs”) supply asset pairs to smart contract pools, traders then swap against these pools at prices determined by a mathematical formula. When a trader submits a swap, the smart contract automatically computes the price and executes the trade, adjusting pool balances accordingly. AMM-based exchanges have seen significant trading volumes, underscoring how AMMs have evolved into an important part of the digital asset marketplace.

SIFMA supports innovation and believes that AMMs, when regulated appropriately, may have benefits to markets. To realize those benefits, the core tenets of technology neutrality, investor protection, regulatory clarity, and consistency with existing market structure frameworks must be applied. Where AMMs support trading in tokenized assets that qualify as securities under U.S. law, U.S. securities regulations should apply.

While AMMs may operate without traditional, centralized intermediaries, this does not eliminate intermediary functions. Rather, those functions are redistributed across developers, governance bodies, liquidity providers, and user interfaces. Accordingly, regulation should focus on the performance of regulated functions, such as facilitating trades, handling customer orders, and determining execution outcomes, rather than the formal designation of any single entity.

Areas Where Design Choices within AMMs May Harm Investors and Markets

The smart contracts that underpin AMMs contain design choices made by their developers. While certain features of an AMM are inherent, e.g., the need for paired liquidity pools, other features are true choices and could be tailored to support outcomes in line with long-standing securities regulations. The emergence of AMM designs were, in large part, due to the constraints imposed by the limited speed and computational power of DLT. Within this section, we discuss where certain features inherent to AMMs may need to be addressed, and how certain design choices could be made to support AMMs regulatory alignment should they trade in tokenized securities.

Design choices

Investor Protections

A unique danger in blockchain-based trading is Maximal Extractable Value (MEV), whereby miners/validators or bots can reorder, insert, or censor transactions in a block to capture profit. This has given rise to "sandwich attacks," a form of front-running in which an attacker sees a pending large trade in the mempool[3] , quickly places their own buy order first in order to drive the price up, then lets the victim's trade execute at the worse price, and finally sells right after to profit on the difference. AMM systems are especially vulnerable because any pending swap broadcast publicly can be exploited by actors willing to pay higher gas fees. This undermines fair execution as retail users may systematically get worse prices than the on-screen quote due to these attacks. In U.S. markets, front-running customer orders is prohibited, and brokers have duties to protect customer order information. Certain AMMs are vulnerable to these risks, such as on-chain front-running, that would be incompatible with securities law expectations, indicating a need for technological solutions (e.g. encrypted mempools, regulatory nodes) or rules that mandate fair sequencing of transactions if AMMs handle securities. Even despite stringent regulations in established equities markets, regulators continue to their work to protect investors by rightly uncovering and charging entities with fraudulent use of material non-public information when trading (*e.g.* in block trades and advance knowledge of large orders), through enforcement of regulations such as FINRA Rule 5270 (Front Running of Block Transactions). Given these risks remain present and need to be actively protected against in heavily regulated traditional markets, the risks are significantly amplified in blockchain based AMM systems where requests/transactions could be publicly visible pre-execution.

[3] Mempool (short for *memory pool*) refers to the collection of unconfirmed transactions that have been submitted to a blockchain network but have not yet been included in a block. Transactions in the mempool are typically visible to network participants and are typically ordered and selected for inclusion based on factors such as their proposed transaction fees and network rules.

These practices would be inconsistent with core U.S. market structure principles, including fair access, best execution, and prohibitions on misuse of customer order information. Accordingly, any AMM-based model supporting securities trading must incorporate enforceable controls that prevent or materially mitigate these practices. Technological architecture does not excuse conduct that would otherwise violate securities laws.

The Commission should also consider how it would evaluate AMM smart contracts to ensure they appropriately protect investors. While it is standard practice in DeFi models to subject smart contracts to security audits, the Commission should review how claimed functionality is evaluated. Without a robust assurance framework, investors would not be protected from claims of functionality that are not reflected in the code itself. In particular, the Commission should consider differences between a narrow security audit, which may identify coding vulnerabilities, and a broader functional assurance review, which assesses whether the protocol in fact performs as represented, including with respect to execution logic, access controls, disclosures, pricing mechanics, and any embedded investor protection or market integrity safeguards. A regime for securities trading cannot rely on audit labels or informal market practice alone. Rather, where AMMs are used to trade tokenized securities, the entities that deploy, maintain, or control those systems should be expected to maintain written policies and procedures, conduct pre-deployment testing, implement controls over system changes, monitor for operational incidents, and assign accountable personnel for systems performance and compliance. Those expectations would be consistent with the principles reflected in Regulation SCI, which requires covered entities to maintain policies and procedures reasonably designed to ensure systems capacity, integrity, resiliency, availability, and security, and to test systems functionality and changes before implementation.

Price slippages should be well disclosed and understood by investors

Unlike traditional markets, where routing, order types, and depth of book mitigate execution risk, AMM pricing is inherently path-dependent and can produce extreme execution outcomes relative to displayed prices. AMMs use formulas that adjust price based on trade size relative to the pool liquidity. Large orders can incur significant slippage (the difference between expected price and execution price) if the pool is small or liquidity is shallow relative to the size of the trade. While users can often set a slippage tolerance, many retail traders may not fully understand this mechanism, leading to large scale losses. Unlike traditional exchanges, where large orders can often be matched at multiple price levels or routed to the best venues, an AMM trade's price impact is determined by the protocol's math. If slippage is excessive, the trade will either execute at a markedly worse price, or fail to execute due to slippage limits, potentially harming investors who may not realize they moved the market against themselves. Disclosure alone is insufficient; structural safeguards are necessary where retail investors are exposed to material execution risk.

The risks these models can present were recently highlighted in a case involving large losses involving the Aave protocol.[4] The March 13 incident saw a user attempt to swap $50.4 million

[4] On March 12th, 2026, a user reportedly lost $49.5 million when using an AMM to swap USDT for AAVE due to the pool's liquidity conditions. See https://finance.yahoo.com/news/aave-crypto-swap-costs-nearly-071133239.html

aEthUSDT[5] for AAVE tokens. The order was routed through a series of DEXs, cascading into one which offered a very shallow pool for the order size. The AMM protocols in question inherently managed large orders against shallow liquidity by causing a major price impact, effectively resulting in a 99% loss for the investor on the swap.[6] While the protocol's interface warned about the possibility of critical slippage, the investor confirmed they had reviewed from a mobile device interface and agreed to the terms, raising questions as to the ability for such "checkbox" disclaimers to adequately warn investors.[7] This swap resulted in the block builder extracting around $34 million in ETH, and a separate MEV bot earning nearly $10 million via a sandwich attack.[8] While an extreme case, this incident highlights a number of areas where certain AMM models in the native crypto space represent structural departures from standards for order routing, execution quality, and disclosures seen in the regulated equities markets.[9]

Unlike conventional equities and options exchanges, post-trade execution quality reporting for AMMs in the native crypto markets is nonexistent. Traditionally, regulators and investors can analyze execution quality (e.g. Rule 605 reports) but assessing whether an AMM-based trade is price-efficient versus a benchmark is more challenging. While public blockchains provide access to this data, further work is needed to create a comparable execution quality report for AMMs. These gaps mean retail users trading securities via AMMs could face hidden costs that erode returns, undermining the investor protection principle of best execution.

The experiences of AMMs supporting the trading of crypto assets call into question the degree to which arbitrage can address pricing issues across venues supported by these models. Theoretically, arbitrage traders can connect prices across AMMs and other markets, but as seen in crypto markets today, this arbitrage is often captured by a small set of sophisticated participants (including bots and high-frequency traders active on-chain). This can concentrate profits in the hands of professional participants and leave retail participants at an economic disadvantage. For instance, when an external market moves, only those with the resources and tools to quickly arbitrage the AMM pool will profit from updating the pool price, while liquidity providers and slower traders may incur losses (e.g., "impermanent loss"[10] for liquidity providers (LPs) when prices fluctuate). LPs in AMMs are uniquely exposed to adverse selection

[5] aEthUSDT is an aToken in the Aave protocol, representing a yield-bearing token that users receive after depositing USDT (Tether) into the Aave V3 Ethereum network. See https://coinmarketcap.com/currencies/aave-ethereum-usdt/

[6] DeFi Trading Error: Trader's $50M USDT Mistakenly Swapped for a Devastating $36K in AAVE. See https://www.mexc.com/news/915867

[7] Investor Loses $50 Million in Token Swap on Aave. See https://forklog.com/en/investor-loses-50-million-in-token-swap-on-aave/

[8] See https://coincentral.com/aaves-50m-defi-swap-disaster-what-went-wrong-with-aave-and-the-crypto-exchange-failure/

[9] Since this incident Aave implemented a new feature designed to block trades when slippage reaches a 25% threshold. This highlights the extent to which disclosures alone are insufficient and need to be supplemented with structural controls. However, even this level of control could still result in investor losses far higher than would be possible in established securities trading infrastructure. See https://www.mexc.co/news/947876

[10] Impermanent loss refers to the risk that liquidity providers may earn less than if they had simply held their assets, due to automatic rebalancing of AMM pools as relative asset prices fluctuate. The loss is unrealized while liquidity remains in the pool but becomes permanent if liquidity is withdrawn while prices remain divergent.

risk, as the sole method to move an "off market" AMM price is to trade against it (and its LPs), unlike traditional markets where participants can update their quotes without intervening executions. A related concern is that market fragmentation, such as the existence of multiple AMMs on different chains or with different designs, can split liquidity, making each pool less efficient and more prone to volatility until arbitrage equalizes prices. If tokenized securities were to trade on several unconnected AMMs, it could impair overall market quality, as liquidity is scattered and price information is not centralized. Thus, while arbitrage can close price gaps, there is a risk of short-term price dislocations and higher trading costs in the interim, especially for less liquid tokens or during periods of market stress.

Innovations in the design of AMMs have sought to address these issues. Concentrated liquidity designs, where liquidity is allocated within a customized price range, allow LPs to allocate capital more efficiently within current market prices. Proprietary AMMs ("propAMMs") similarly allow LPs to place liquidity within a price range, which is then continuously updated, typically via an off-chain pricing feed. As the Commission explores the possibilities of AMMs supporting tokenized securities, it will be essential to take a close and critical look at the design features of any potential AMMs to be adopted, to ensure that they embed the necessary controls to address these issues and avoid the departures from the standards of established equity trading venues seen in many AMMs supporting the crypto markets. This should also include a review of the process by which transactions are routed to any future tokenized securities trading AMMs, and the appropriate disclosures and controls around that order routing, a question SIFMA previously discussed in our prior letters on wallet providers and their role in routing to different AMMs. [11]

Price Discovery and post-trade price transparency

U.S. equity markets rely on consolidated quoting and reporting (the National Best Bid and Offer ("NBBO") and trade tape) to ensure that price discovery is robust and transparent across venues. By contrast, most AMM trading occurs in siloed liquidity pools on separate blockchains or platforms, without any reporting to a consolidated tape. Prices on an AMM are determined by the local liquidity pool's conditions and may diverge from the broader market price of an asset. If a token trades on multiple AMMs, or on an AMM and a centralized exchange, there are typically no built-in mechanism to keep those prices aligned beyond arbitrage actions. This raises concerns about fragmented price formation, especially for tokenized securities that might trade in both traditional venues and AMMs.

As discussed in our response to Commission Peirce's "And Then Some"[12] RFI, a key question is how Regulation NMS would apply. Currently, Regulation NMS assumes USD pricing and conventional trade reporting. As such, a tokenized security trading in an AMM against a cryptoasset falls outside its scope. If AMM venues were to be integrated, they would need to report quotes and trades into the

[11] vis. SIFMA's discussion of the obligations of wallet providers who are facilitating tokenized securities transactions in our January 15 and February 27 letters to the SEC. See https://www.sec.gov/files/sifma-follow-wallet-letter-022726.pdf (Feb 27, 2026) and https://www.sec.gov/files/sifma-letter-wallet-provider-regulation-011526.pdf (Jan 15, 2026).

[12] See SIFMA's response to the "And Then Some RFI" https://www.sec.gov/files/ctf-written-sifma-ats-rfi-letter-03-17-2026.pdf (Mar 17, 2026)

national market system, e.g. to SIPs or trade reporting facilities[13], just like any other exchange or ATS. The absence of such reporting would mean investors would lack reliable post-trade price transparency on DeFi trades, and regulators would not be able to easily monitor pricing across dispersed pools. This opacity could impair price discovery and complicate best execution obligations if broker-dealers execute client orders on or alongside AMMs. The Commission should consider how AMM models could be integrated into existing price and reporting requirements, and how to achieve that consistently given divergences between price and quote models between AMM models and NMS infrastructure. Absent integration into consolidated quoting and reporting frameworks, AMM-based trading of securities could impair both price discovery and the ability of broker-dealers to satisfy best execution obligations.

If AMMs rely upon oracles to provide pricing data to support their automated trading models. A potential risk factor is presented if the sources of these market data are not held to high standards for reliability, security, and accuracy. Indeed, there have been a number of recent incidents where operations within decentralized exchanges ("DEXs") were disrupted by errors or fraud affecting the oracles providing their pricing. In March 2026, Aave's pricing oracle priced a product at ~3% below its actual market price, triggering a wave of ~26 million in liquidations as some leveraged borrowers' positions appeared undercollateralized.[14] Oracles supporting AMMs have also been the targets of manipulation to enable fraud. In April 2025, the KiloEx exchange was targeted by attackers who manipulated the pricing data the oracle relied on to execute mispriced swaps in its AMM.[15] Similarly, in 2022, Mango Markets oracle was disrupted by a trader carrying out large parallel trades to fraudulently manipulate pricing.[16]

In our prior letters, we discussed the importance of consistently integrating pricing data for tokenized securities trades executed on any alternate models or trading platforms into the broader market data infrastructure on a consistent, timely, and accurate basis. Ensuring that any alternative trading models draw their pricing inputs from sources that accurately capture broader market prices (where applicable) and meet high standards of resiliency will be critical. Addressing these challenges can help ensure that any AMM adoption meets the high standards for market price integration seen in the established equities markets.

Unvetted Pseudonymous Trading

A defining feature of public blockchains is open, pseudonymous access, allowing users to transact without identity verification. This contrasts sharply with regulations in securities markets that

[13] As further discussed in our response to the ATS RFI, reporting to the SIP requires an ATS to be a regulated exchange, and reporting to TRFs requires FINRA membership.

[14] Aave users lose $26M after wstETH oracle misconfiguration triggers liquidations. See https://cryptobriefing.com/aave-wsteth-oracle-misconfiguration/

[15] Explained: The KiloEx Hack (April 2025). See https://www.halborn.com/blog/post/explained-the-kiloex-hack-april-2025

[16] Mango Markets Exploit – Detailed Analysis. See https://immunebytes.com/blog/mango-markets-exploit-oct-11-2022-detailed-analysis/

require brokers to Know Your Customer ("KYC") and enforce anti-money-laundering ("AML") rules. This stands in direct tension with core securities law requirements that rely on identifiable participants to enforce AML, sanctions compliance, and market integrity rules. Open access to certain trading platforms combined with pseudonymous nature of blockchain addresses means that bad actors can potentially engage in, or intermediate, securities transactions on AMMs outside of the Bank Secrecy Act and AML oversight that applies to broker-dealers and exchanges. This raises not only money-laundering and sanctions evasion worries, but also market integrity issues. For example, one individual or coordinated group can create multiple wallet addresses and use them to evade position or participation limits, manipulate governance (in protocols where voting power is based on tokens) or markets. Instances of wash trading, where a user artificially trades with themself to boost volume or manipulate price, are harder to detect when the trader can mask their activity behind various addresses with no central registry of beneficial owners. Within a regulated exchange, in contrast, accounts are tied to verified identities, and surveillance software can often detect and aggregate related accounts or suspicious trades.

In AMMs which lack access controls or vetting of participants, even though every transaction is visible on the public ledger, identifying the actors behind them is challenging, and real-time intervention is nearly impossible. This stands in contrast to securities markets, where regulatory requirements are often enforced through intermediaries even when the issuer or seller is not directly regulated. For example, Rule 144 imposes conditions on public resales of securities by affiliates, and those conditions are operationalized and enforced through the brokers facilitating the sale, including restrictions on manner of sale, volume, and disclosure. By comparison, most AMM implementations lack an intermediary with the ability or obligation to enforce comparable transaction-level controls. There have been efforts to "permission" AMMs, e.g., pools that only allow known wallets to trade or provide liquidity. But so far, most platforms only implement light forms of permissioning, typically by allow-listing LPs, and allow essentially unrestricted trading on the user side. This means that key regulatory safeguards, such as prevention of insider trading and market manipulation are difficult to enforce, since identifying the perpetrator in an anonymous setting is a significant hurdle. The Commission should consider how a regulatory framework might need to address how AML/KYC requirements could be applied to AMM-based systems, for instance, through regulated wallets that provide access or through recognition of compliant "allow-listed" pools.

Market Manipulation Controls

In contrast to regulated markets, there is no embedded mechanism within most AMMs to detect, prevent, or halt manipulative activity in real time. Traditional exchanges and intermediaries employ extensive measures to detect and prevent manipulative trading, including surveillance systems that flag suspicious patterns (like wash trading or spoofing), circuit breakers to halt trading during extreme volatility, and rules against self-dealing. AMM platforms, by contrast, lack built-in surveillance or automated controls to curb manipulation. There are no provisions for circuit breakers in most AMM smart contracts. Trading continues irrespective of a rapid price crash, unless an external party, such as a governance vote, intervenes; an intervention that would not be in real-time. Cross-venue manipulation e.g., using one pool to signal or influence prices in another is feasible and generally unmonitored. Without

an overarching surveillance authority, malicious actors could exploit AMMs to paint misleading price pictures. For example, users could rapidly swap tokens back-and-forth to create a high volume and price spike intended to trick oracle systems or traders. Indeed, unregulated platforms could engage in "tape painting," injecting bogus quotes or trades into public data feeds if those feeds were linked to AMMs. The lack of real-time cross-market oversight means activities that would be prohibited in equities markets may go undetected on AMMs. This not only holds the potential to harm market participants and could also undermine confidence if such venues were to play a larger role in securities trading. Addressing these risks would require integrating AMM-based trading into surveillance frameworks comparable to those applied to exchanges and broker-dealers.

AMMs may be "non-upgradable" or subject to continued development

The smart contracts underpinning AMMs may be designed as "non-upgradable," meaning that once deployed, the developers/deployers of those contracts are no longer able to make changes to the code. Alternatively, via the use of proxy contracts, AMMs could enable continuous upgradability. These two models raise distinct but important questions: if the AMM can be continuously modified by its deployer, that deployer retains ongoing control over the trading system's functionality, parameters, and risk profile, which is analogous in many respects to the role played by an exchange or other regulated trading venue. In such cases, the ability to change pricing logic, access rules, fee structures, or trading mechanics over time suggests the presence of an accountable operator (or consortium thereof) with responsibility for the system's operation. By contrast, a genuinely non-upgradable AMM raises different questions regarding accountability, governance, and regulatory responsibility, particularly where no party has the ability to remediate errors, respond to market stress, or implement investor protection controls.

In addition to the question of upgradability, certain AMM models may have "administrator-only" functionalities. In these cases, parameters may be updated by the use of an administrator key, while the underlying code itself is not subject to change[17]. The Commission should consider how differing upgrade and control models affect the allocation of regulatory obligations and the identification of responsible parties when AMMs are used to trade tokenized securities. Where a person or group retains the ability to modify core trading parameters or operating rules over time, that degree of control should be a key factor in determining whether the AMM operates as a regulated trading system rather than as a technology platform. Relatedly, securities trading on a non-upgradable AMM may present risks given its lack of updated cyber and resiliency controls or processes to manage technical or operational disruptions.

Role of the Liquidity Provider in AMMs

In traditional markets, market makers are subject to market-making rules and oversight. They are typically registered broker-dealers and must adhere to capital requirements, reporting, and rules against front running and other manipulative practices. By contrast, in most AMMs, anyone can be an LP, and

[17] For example, in early 2026 the Uniswap community approved governance proposals authorizing changes to core protocol parameters, including the activation and expansion of protocol-level fees across multiple liquidity pools and networks. These changes were approved through token-holder voting and implemented through on-chain governance mechanisms, demonstrating that, notwithstanding claims of decentralization, key economic and operational parameters of an AMM in these models can be modified over time by identifiable governance processes rather than being fixed at deployment.

there are no affirmative obligations or fiduciary duties to the market or other participants. An LP can withdraw liquidity at any time, even during volatile periods, potentially exacerbating price swings (equivalent to a market maker leaving the market in a tumult, an activity that is monitored in traditional markets and where the responsibilities of the market marker are defined). LPs profit from trading fees and can also benefit from price movements in the pooled assets yet face no specific restrictions on using non-public information or on conflicts of interest. For example, an LP who knows that a large trade is forthcoming (perhaps the LP themself plans to initiate it via another wallet) could pull their liquidity beforehand to avoid being adversely selected, an action that would be akin to a market maker stepping away right before a big customer order (in traditional markets, there are punitive consequences for this to discourage/prevent). There are no rules preventing an LP from engaging in such strategic liquidity withdrawal, whereas a designated market maker on an exchange might be constrained by obligations to maintain orderly trading.

Some permissioned liquidity pools exist where only allow-listed institutions can provide liquidity, which more closely resembles a prime dealer system, but these are exceptions. Generally, LPs operate free of the kind of regulatory oversight applied to analogous roles in traditional markets, representing a regulatory gap. As LPs essentially trade on their own account as counterparts to investors and may set pool parameters that affect pricing, potential conflicts of interest can arise. In securities markets, by contrast, market makers and dealers have obligations (e.g., FINRA rules on fair prices, best execution when filling customer orders as a dealer, etc.). This divergence suggests that a regulatory framework for AMMs must consider imposing certain obligations/penalties on significant LPs or ensure they are registered and supervised as dealers when dealing in securities, to align incentives with market integrity.

These issues are further complicated by a lack of clarity regarding the legal capacity in which AMM participants operate. Traditional markets operate on a well-established distinction between agency and principal capacities. When a retail investor interacts with an AMM liquidity pool, it is unclear whether the pool, the protocol, or the LPs are acting as principals (dealers taking the other side of the trade) or agents (facilitating exchange between parties). This distinction is critical because it determines risk allocation: in an agency capacity, execution risk typically remains with the investor, while in a principal capacity, the dealer bears execution risk, and the investor has recourse if obligations are not fulfilled. It also determines disclosure requirements, fiduciary duties, and best execution obligations. In contrast, trading on AMMs does not clearly define these roles, or align them with the kind of mandatory disclosure regarding the capacity in which AMM counterparties are operating. These ambiguities would need to be resolved and the roles of participants on AMM-based trading clearly aligned with the regulatory responsibilities of different roles of market participants to support securities trading at the consistent standards of investor protection and market integrity.

Order Types & Market Conventions

Securities markets have a rich variety of order types (limit, market, stop-loss, etc.) and standardized conventions such as tick size increments, round lot sizes, and opening/closing auctions, many of which are absent or fundamentally different in AMMs. In an AMM, trades are typically executed

immediately at the prevailing algorithmic price, and the concept of a resting limit order is not native to basic AMM designs (though users can approximate limit orders using external smart contracts or by adjusting slippage and transaction timing). No concept of bid-ask spread exists in the traditional sense, the "spread" is instead a function of pool liquidity and the trade size. Tick size in cash equities ensures uniform quoting granularity, whereas AMM prices are essentially continuous since they derive from ratios.[18] These differences can cause friction in integrating AMMs with existing market systems.

Inherent Features of AMMs

The technical constraints of DLT

As discussed in the onset of this section, AMM designs were influenced by the environment in which they are deployed. As many DLT ledgers operate at slow speeds (when compared to traditional compute infrastructures), and require gas fees to pay for that compute, AMMs were designed to take advantage of models which required infrequent updates. When compared to dynamically updated closed limit order books, which update frequently, the algorithmic pricing models that underpin many AMMs allow for less compute intensive operations.

These design choices, while technically efficient in a blockchain context, introduce meaningful tradeoffs if applied to securities markets. Formulaic pricing updates only when trades occur, rather than through continuous quote updates, can result in stale prices, greater price impact for larger orders, and reliance on arbitrageurs to realign prices with broader market conditions. Similarly, batching transactions into blocks and executing them without strict price-time priority departs from core market structure principles that underpin fairness, transparency, and best execution in U.S. securities markets.

As a result, certain features often described as "inherent" to AMMs may be better understood as responses to current DLT constraints rather than as unavoidable characteristics of trading systems. If AMMs are to support the trading of tokenized securities, regulators should critically assess whether these constraint driven design compromises are appropriate for securities markets, or whether alternative architectures and controls are necessary to meet established investor protection and market integrity standards.

Error and dispute handling

Within conventional markets, if a trade error occurs, there are established processes for resolving disputes or cancelling trades. The absence of an accountable intermediary within typical AMM models means investors may have no resource/pathway to resolve losses from technical failures or exploits or are they can only access limited, discretionary, and often ex post mechanisms rather than standardized, operator-administered error resolution, unless the governance of the protocol chooses to intervene (which

[18] The Commission should consider how rule 612's requirements for tick sizes in NMS securities would apply in this context. While it may be theoretically possible to round AMM outputs to the nearest permissible tick, doing so would introduce discontinuities between the AMM's internal pricing curve and executable prices. Imposing discrete tick-size rounding on such continuously adjusting prices could introduce systematic rounding gaps between on-chain AMM prices and prices available on other venues, creating predictable arbitrage opportunities unrelated to underlying supply and demand. These effects could undermine both the objectives of Rule 612 and the integrity of algorithmic pricing mechanisms used by AMMs.

may be technically impossible or may subject it to securities laws that it has been exempt from up to that point). This lack of a reliable dispute resolution mechanism and responsible party is a significant investor protection gap. Technology does not absolve the obligation to safeguard investors, if a trading platform uses code, it should undergo rigorous audits (covering both security and functionality) to ensure the code behaves as intended. Moreover, any compliance or market rules automated via smart contract still need a human or firm accountable for their correct execution. Currently, AMM protocols rarely undergo the kind of formal regulatory compliance checks that are required within an exchange's system, e.g. SEC Rule SCI requires exchanges to have policies to ensure technical stability and prompt issue resolution. The risks that this lack of error resolution procedures presents to investors was highlighted in the March 2026 Aave liquidity slippage incident discussed above, where the investor in question had no recourse, other than the voluntary refunding of transaction fees by the platform.[19]

Liquidity issues

AMMs require a significant volume of capital to be locked in liquidity pools to support trading activity and maintain price stability. This capital requirement, where both sides of a trading pair must be pre-funded, can limit the scalability of AMMs and restrict the range of viable trading pairs. In practice, only highly liquid tokens tend to attract sufficient liquidity to support meaningful trading, which may bifurcate markets and exclude less liquid securities from participating in AMM-based trading models. Moreover, the fragmentation of liquidity across multiple AMMs, as they are often deployed across different blockchains and multiple AMMs compete for liquidity within the same blockchain, can exacerbate inefficiencies. The Commission must holistically consider the liquidity impacts to U.S. securities markets that would arise should they be integrated within AMMs. Of note, regulated financial institutions possess significant liquidity in securities that may, in the future, be tokenized. Clear and durable regulations would enable those institutions to participate in AMM based models, greatly enhancing the liquidity on offer to AMMs.

Consistent Regulation of Exchange / Broker Functions in AMM-supported Markets

As the Commission considers the possibility of AMM-driven models for the trading of tokenized securities, it is critical to consistently apply regulatory requirements to entities whose roles in these markets are substantively like exchanges, brokers, market makers, or other regulated functions. We recognize that there is a diversity of AMM models in the non-security crypto markets, and the roles and responsibilities of the various technological and operational functions that support them vary between markets and platforms. Foundations, developers, DAOs, and front-ends play different roles in supporting trading in different protocols. However, this complexity should not deter regulation from being

[19] Crypto investor turns $50 million into $36,000 in one botched move. See https://www.coindesk.com/markets/2026/03/12/crypto-investor-turns-usd50-million-into-usd36-000-in-one-botched-move

consistently applied to those entities whose activities in AMM-driven markets meet the definition of an exchange or ATS.[20]

As discussed above, it is critical to differentiate AMMs themselves – as bundles of smart contract code – from the entities that deploy them or support customer interactions in the markets they are deployed in. Smart contract code is not a registrable "person" and cannot independently satisfy regulatory obligations under the federal securities laws. While persons who deploy, upgrade, or control the code may collectively satisfy Section 3(a)(1) (depending on the nuances of how those actions are handled), code by itself cannot register or comply with Section 6 or Regulation ATS, nor can code monitor for, and update itself to address, changes in applicable law. Instead, the regulatory requirements of an exchange should attach to the organizations whose activities in deploying and operating AMM-supported markets align with the statutory definitions of an exchange or ATS. This will likely mean regulatory requirements of an exchange attach to certain developers and foundations who build, deploy, and operate AMM-driven markets and / or front-end platforms who support investors' interactions with those markets.[21]

As observed today, many AMMs are supported and managed by foundations and governance bodies who play an active role in their operations equivalent to the definition of an exchange and/or ATS. While there are differences in how this oversight is executed across platforms depending on the roles of foundations and DAOs, there are clear examples where they provide ongoing technical support, governance, infrastructure development, and management of the listings and economic parameters that are clearly aligned with the role of an exchange operator or ATS, not merely a software developer. Were these platforms to support tokenized securities trading, they would need to be regulated as an exchange or ATS.

We recognize that there are models where the foundations which develop AMM-supported trading protocols release them without offering any on-going support, as discussed above. This model complicates the relationship between the technology itself, and managerial oversight seen in definition of exchanges and ATSs. It also raises serious questions on the risks presented by tokenized securities trading that occur on platforms that lack any ongoing support and maintenance. This would be a structural departure from established models of securities trading, where exchanges and ATSs have clearly defined regulatory responsibilities to support the ongoing technological and operational resilience of the software and systems they use to execute transactions (e.g. Reg SCI and cybersecurity regulations). There are obvious investor protection and market integrity concerns if securities trading occurs on platforms that

[20] We note that an ATS is a trading system that meets the definition of exchange under federal securities laws but is not required to register as a national securities exchange if it operates under the exemption in Rule 3a1-1(a). To use that exemption, it must register as a broker-dealer and comply with Reg ATS.

[21] We recognize that there are ongoing legislative and policy discussions around when code enabling on-chain markets is "deployed" and the specific regulatory responsibilities associated with those entities or persons who are involved in the development of code as opposed to its deployment, and ongoing supervision and operations of platforms which are based on that code. The focus of this letter is on circumstances where code has been deployed and is a platform based on it is actively being managed by an entity to support securities trading

have no ongoing managerial functions to handle resiliency management, cybersecurity oversight, and dispute resolution or recourse provisions.

We encourage the Commission to explore the role of front-ends, and in particular whether there are combinations of services which front-ends offer to clients which would establish them as serving as exchanges or brokers. There are diverse models of front-ends, and as SIFMA discussed in our prior letters on wallet providers, it is important to develop a clear process to establish when the combination of services they offer moves them from being simple technology support providers that facilitate trading to meeting the definition of exchange. These include exchange-like features such as off-chain order handling, curated order interaction rules, or interface-level fee structures tied to execution. Indeed, looking at models seen in the native crypto markets there are a number of front-ends who combine those services, and should be regulated as exchanges if they were to support tokenized securities trading. Where front-ends curate execution, route orders, or influence trading outcomes, they perform functions that are indistinguishable from those of brokers or exchanges.

However, there are other front-ends whose role is confined to a more technical support capacity, such as assisting users in composing transactions. In these models, the front-end "composes" a transaction to a format which can be accepted by the network, but the ultimate transmission and execution of the trade occurs through the users' wallet and RPC node which provides a point of contact to a peer-to-peer network. Nor is the front end necessary for interactions with protocols, with many larger or more sophisticated users bypassing front-ends entirely. Were these models to be adopted for securities trading, it would be necessary for the Commission to develop a framework to clearly and consistently identify when front-end activities rise to the level of exchange or ATS functions and need to be regulated as such, and when they act in a technical support function. This regulatory clarity will help ensure consistent application of regulatory protections for investors and markets.

Regulatory responsibilities of liquidity providers in AMM-support tokenized securities markets should also be considered. As discussed above, the role of liquidity providers in AMM markets has many similarities to those of market makers, though without the corresponding regulatory obligations. Given the potential for conflicts of interest and disruptions to market stability, extension of broker or market marker requirements may be necessary for some liquidity providers in AMM markets in tokenized securities. AMM markets differ from traditional securities markets in that frequently there is no lower bound on the volume of assets that liquidity providers can contribute, rulemaking in this area may need to differentiate between small liquidity providers from those operating on a scale that their behavior can influence the markets they operate in. We encourage the Commission to look at these issues and ensure that treatment of liquidity providers results in consistent standards and outcomes in terms of investor protection and market integrity.

Historical Precedents Show That Technologies Can Advance and Automation Can Develop Under the Regulatory Umbrella

Equity markets have a long history of embracing technologies to eliminate frictions in the trading ecosystem. The first generation of automated liquidity engines can be traced back to the early 1990s. Automated market making systems at Shearson Lehman Brothers and Automated Trading Desk (ATD) marked early attempts to operate automated quoting and execution systems, which generated automated quotes, updated prices continuously based on market data feeds, executed trades electronically, and utilized deterministic logic to continuously make markets in U.S. equities. This is one of many examples where participants in equity markets sought out technologies to introduce efficiencies, such as reducing latency, scaling liquidity provisioning, and providing tighter spreads.

The 1990s were considered the beginning of modern algorithmic trading, and the Shearson Lehman and ATD systems were precursors to algorithmic market making. Granted, there were not AMMs as we know them today. These systems were not decentralized, permissionless, or formula-driven, rather early examples of automating dealer functions. These systems also differed in an important way from today's AMMs. Shearson Lehman and ATD were registered, fully regulated entities.

The first examples of automated market making systems in U.S. equities were built inside the broker-dealer regulatory perimeter, not exempt from registration simply because of the technology or automation. Equity markets have always identified the path to incorporate new technologies into the regulatory environment.

Key Policy Recommendations

SIFMA believes the Commission should maintain technology neutrality by regulating AMMs based on their market function rather than protocol architecture and explicitly recognize that "decentralized" execution often shifts rather than eliminates intermediary functions such as order routing, execution, and custody transfer.

In particular, we recommend the Commission:

- Define and allocate regulatory responsibility across the AMM ecosystem by mapping obligations to distinct functional roles (e.g., protocol deployers and governance bodies, significant liquidity providers, and user interfaces such as wallets and DEX aggregators) and specify the circumstances under which each role triggers exchange, broker dealer, dealer, or other requirements.
- Apply investor protection expectations at the points where investors interact with AMMs by requiring clear, prominent disclosures regarding slippage, execution mechanics, and MEV related risks, and by applying broker-like standards (including best execution) to interfaces that route, curate, or otherwise influence execution.
- Establish robust price discovery and post-trade transparency by providing a pathway for AMM venues that trade tokenized securities to report quotes and transactions into the national market

system (or a comparable reporting construct), and by specifying how Regulation NMS concepts apply where tokens are priced, traded, and settled on-chain.

- Maintain market integrity protections notwithstanding automation or pseudonymous access by specifying how surveillance, manipulation controls, and AML/KYC expectations apply when tokenized securities are traded via AMMs, including consideration of compliant permissioned/allow-listed access models and the role of regulated wallet providers or other access points.
- Require strong operational resilience and systems integrity for AMM-based trading in securities by specifying how principles analogous to Regulation SCI, code audit expectations, and incident response and dispute handling obligations should attach to the entities that deploy, maintain, or materially upgrade trading-related smart contracts.
- Affirm that the use of decentralized or automated technology does not alter the applicability of securities laws where regulated functions are performed.

Conclusion

AMMs represent a technological variation in how trading functions are implemented, not a departure from the underlying economic roles those functions perform. Federal securities laws regulate functions, bringing together buyers and sellers, facilitating execution, and providing liquidity, not the specific technology used to perform them.

The Regulatory oversight of AMMs should be cognizant of how common operating models seen in the native crypto markets represent structural departures from the models of established securities trading infrastructure. These have clear, and in many cases negative, implications for investor protection and market quality. At the same time, it is important to distinguish between troubling features of AMMs seen today which represent design choices by their operators and those which are inherent in their operating model. Any path forward for the integration of AMMs in trading of tokenized securities will need to incentivize design choices which result in comparable standards for investor protection and market integrity to established markets. A technology-neutral approach that applies existing regulatory frameworks to these functions will allow innovation to proceed without compromising the core principles of investor protection, market integrity, and fair competition.

*****

We look forward to continuing to engage with the Commission as it works through these complex issues. Please feel free to contact Peter Ryan (pryan@sifma.org) or Charles De Simone (cdesimone@sifma.org) with any questions regarding these comments.

Sincerely,

Kenneth E. Bentsen, Jr.

CEO and President

Securities Industry and Financial Markets Association

Cc: Jamie Selway, Director of Division of Trading and Markets

Appendix I - Aligning AMM-based Operating Models with those in Established, Regulated Markets

In this letter and in SIFMA's prior letters, we recommend the Commission focus on analyzing the economic functions and legal responsibilities which underpin on-chain operating models and use those as the foundations for determining if and how securities regulations should be applied. This focus on concrete roles and responsibilities as opposed to technological configurations is more likely to result in a consistent regulatory outcome and prevent opportunities for regulatory arbitrage.

To this end we would like to highlight in the tables below an illustrative analysis of how certain AMM-based operating model configurations could align with the roles of exchanges, brokers, and market makers as seen in established markets and defined through regulation. While these tables are simplified, they illustrate a clear point – that many AMM-based models contain within them exchange or broker activities were they to be applied to trading tokenized securities.

As discussed above, there are a great diversity of AMM-based operating models and the charts are reductive to illustrate points of alignment. Developing actual regulatory frameworks for AMM-based models would require a facts and circumstances analysis of specific operating models.

AMM-based Trading Platforms Functionality & that of Exchanges

AMM definition: An AMM is a decentralized exchange trading mechanism that facilitates the buying and selling of digital assets through liquidity pools and deterministic pricing algorithms, rather than through a traditional order book. In an AMM, users supply assets to a pool, and trades occur directly against that pool at prices set by a predefined mathematical formula, with no discretionary intervention by an operator.

Exchange definition:[22] The Exchange Act defines an exchange as any organization, association, or group of persons which constitutes, maintains, or provides a marketplace or facilities for bringing together purchasers and sellers of securities and for executing trades according to established, non-discretionary rules.

AMMs often differ in how prices are formed, liquidity is supplied, and trades are executed. However, whether an AMM or a "traditional" equity exchange, the two models both match buyers and sellers, just with different underlying micro market structure.

Function	AMMs	Exchanges

[22] It has been argued that AMMs may be more aligned with ATSs. Should that be the route the Commission chooses to take, we note that an ATS is an exchange. An ATS is a trading system that meets the definition of exchange under federal securities laws but is not required to register as a national securities exchange if it operates under the exemption in Rule 3a1-1(a). To use that exemption, it must register as a broker-dealer and comply with Reg ATS.

Brings together orders of multiple buyers and sellers	Liquidity pool aggregates all trading interest	Aggregation of trading interest
Uses non-discretionary methods for order interaction	Uses deterministic pricing formula	Set rules and matching engine
Price setting	Algorithmic, price is set by a formula and arbitrage	Market driven, price emerges from order book interaction
Trade execution	Automatic, swap executes directly against pool	Automatic, matching engine executes orders
Liquidity provision	LPs supply pooled inventory, AMM rebalances automatically	Designated market makers (formerly called specialists)
Operator/Regulatory Status	None in decentralized form, DAO/front end may be deemed operator; unregistered exchange	Registered exchange (and Self-Regulatory Operator/SRO)

Note: Again we note that an ATS is an exchange, operating under an exemption, registered as a broker-dealer, and complying with Reg ATS.

Liquidity Providers' (LPs) Functionality & that of Dealers

LP definition: A LP is a participant who supplies assets to an AMMs' liquidity pools, enabling the system to execute trades against that pooled inventory, swapping against these pools at prices determined by a mathematical formula. When a trader submits a swap, the smart contract automatically computes the price and executes the trade, adjusting pool balances accordingly. In return, the LP earns a share of trading fees and assumes the economic risk associated with price movements and rebalancing within the pool.

Dealer definition: The Securities Act and Exchange Act define dealer as any person engaged in the business of offering, buying, selling, or otherwise dealing in securities issued by another person.

Transacting definition: While not a single defined term in the Exchange Act, transacting in a security involves changing beneficial ownership of a security for value.

Market maker definition: The Exchange Act defines a market maker as a dealer who, with respect to a security, holds itself out as being willing to buy and sell that security for its own account on a regular or continuous basis.

While the underlying micro market structure again differs, the functions of liquidity providers on AMMs and dealers broadly overlaps.

Function	LPs	Dealers
Buys and sells securities	Yes, an AMM continuously buys and sells on LP's behalf	Yes

Acts for its own account	Yes, LP's assets are the trading inventory	Required
Regular business/ continuous activity	Yes, an LP is continuously standing ready via the pool	Required
Holds itself out as willing to buy and sell	Functionally yes, AMMs advertise two-sided liquidity	Required, core dealer function
Liquidity provision	Yes, an LP's inventory is used to fill customer trades	Yes
Discretion over pricing	None, AMMs set price algorithmically	Dealers may quote or adjust prices
Assumes market-making risk	Yes, impermanent loss, adverse selection, inventory risk	Yes, inventory and price movement risk
Earns transaction-based compensation	Yes, an LP earns a pro rata share of trading fees	Yes, via spreads
Operator/Regulatory Status	Not registered; no outside/regulatory oversight	Registered with SEC and FINRA