MEMORANDUM

To:	Crypto Task Force Meeting Log
From:	Crypto Task Force Staff
Re:	Meeting with Representatives of Superform Labs and Manatt, Phelps & Phillips LLP

On February 17, 2026, Crypto Task Force Staff met with representatives from Superform Labs and Manatt, Phelps & Phillips LLP.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Superform Labs and Manatt, Phelps & Phillips LLP representatives provided the attached document, which was discussed during the meeting.

Subject: Follow-Up Meeting Request - Non-Custodial Yield Infrastructure Regulatory Framework

Dear Crypto Task Force,

Thank you for the productive discussion at last week's SEC roundtable in Miami. We appreciate the Commission's continued engagement with the digital asset industry and its focus on developing clear regulatory guidelines for founders, builders, investors and consumers.

Following that conversation, Superform would like to request a follow-up meeting with the Crypto Task Force to discuss potential pathways for regulatory clarity around non-custodial onchain yield infrastructure. Specifically, we're seeking guidance on no-action relief, exemptive relief, or input that could inform rulemaking on a conditional safe harbor for non-custodial financial applications.

As discussed at the roundtable, Superform operates as the first user-owned neobank - a non-custodial application that provides users access to yield-generating vaults and DeFi opportunities across multiple blockchain networks. We never hold user funds, do not execute transactions on users' behalf, and have no discretionary control over assets. Users maintain full self-custody through their own wallets and sign all transactions directly. We believe our model presents an opportunity to establish user protection standards without applying traditional custody-based regulatory frameworks that don't fit the technology.

We've prepared a brief overview (attached) outlining:

- How non-custodial yield aggregators function as pure software interfaces
- Key distinctions from traditional intermediaries and custodial services
- Disclosure and transparency standards we've developed through rigorous auditing
- A potential framework for a narrow, conditional safe harbor
- Section 230 analogies as precedent for platform liability principles

We would welcome the opportunity to share our technical architecture and discuss how Superform can help the Commission develop disclosure standards that work for this technology to protect consumers while unleashing American innovation. Our team has invested significant resources in security audits, validator attestation systems, and user protection mechanisms, and we're eager to work collaboratively toward appropriate regulatory guardrails.

Proposed attendees from Superform:

Vikram Arun, Superform

Blake Richardson, Superform

Mike Katz, Partner, Manatt, Phelps & Phillips LLP

We're flexible on timing and format - happy to meet in person or virtually at the Task Force's convenience over the next few weeks.

Thank you for your consideration. Please let us know if you need any additional information.

Best regards,

Vikram Arun

Superform

ATTACHMENT: MEETING OVERVIEW

NON-CUSTODIAL YIELD INFRASTRUCTURE: REGULATORY FRAMEWORK DISCUSSION

Background

Superform is the first user-owned neobank, providing users with non-custodial access to yield-generating opportunities across multiple blockchain networks. Through our platform, users can access over 1,200 earning opportunities across leading DeFi protocols including Pendle, Morpho, Aave, and Euler. With over 180,000 lifetime depositors, $70 million in total value locked, and zero security incidents, Superform has established itself as a leader in making institutional-grade yield accessible to everyday users.

Unlike traditional financial intermediaries or even centralized crypto platforms, Superform never takes custody of user assets, does not execute transactions on behalf of users, and exercises no discretionary control over funds. Users maintain complete self-custody through their own wallets and sign every transaction directly on-chain.

Following our participation in the SEC's recent roundtable discussion, we are seeking guidance on establishing regulatory clarity for non-custodial onchain applications through:

- No-action relief confirming applicability (or non-applicability) of securities laws
- Exemptive relief under appropriate statutory authority
- Input to inform potential rulemaking on a conditional safe harbor framework

Key Characteristics of Non-Custodial Onchain Applications

Non-custodial yield platforms like Superform function fundamentally differently from traditional financial intermediaries:

Pure Software Interface, Not Financial Intermediary

- Users always maintain unilateral control of their assets via self-custody wallets
- All transactions are signed and executed directly by users on-chain
- Superform provides discovery, comparison, routing information, and interface infrastructure only
- No pooling of assets, no omnibus accounts, no custody whatsoever
- Modular smart account infrastructure (ERC-7579) enables users to interact with complex protocols while maintaining full control, and users can bypass Superform entirely to interact with underlying protocols directly

No Discretionary Management or Execution Authority

- Users make all investment decisions independently
- Superform does not provide individualized investment advice
- No asset management, portfolio construction, or discretionary rebalancing services
- Platform displays available vault options; users independently select and execute

Analogous to Financial Information and Routing Platforms

- Similar to how Bloomberg provides financial data aggregation or Kayak aggregates travel options
- Information curation, comparison tools, and transaction routing, not transaction execution
- Users interact directly with underlying DeFi protocols via their own wallets
- Superform facilitates discovery and simplifies technical complexity but does not intermediate the relationship between user and protocol

Built on Audited, Transparent Infrastructure

- Multiple independent security audits (Spearbit,, Cantina, 0xMacro, GetRecon, Nodesec) and continuous ongoing security through Octane, Tenderly, and Hypernative.
- All protocol updates, fee structures, and strategy changes published on-chain
- Users can verify exact routing, fees, and destinations before signing any transaction

Accountability Framework Without Traditional Custody Regulation
While Superform does not fit traditional custody or advisory models, we recognize responsibility for:

Risk Disclosures

- Clear presentation of smart contract risks, protocol risks, underlying vault strategies
- Yield volatility warnings and historical performance context
- Security audit status and validator attestations displayed prominently
- Technical complexity indicators and user sophistication requirements
- Jurisdictional restrictions and compliance limitations

Conflict-of-Interest Disclosures

- Transparent disclosure of all fee structures and revenue arrangements
- Clear labeling of protocol relationships and economic incentives
- Distinction between protocol-level fees and Superform-level fees
- Validator and strategist staking requirements to align incentives
- No hidden fee structures or opaque execution practices

Routing and Algorithm Transparency

- Explanation of how vault options are selected, filtered, and ranked
- Disclosure of any economic incentives affecting vault placement or routing decisions
- User control over filtering, sorting, and selection criteria
- Open-source hooks system allows composable transaction flows

Product Labeling & Interface Standards

- Accurate protocol names, vault strategies, and risk categories
- Prohibition on misleading yield projections or guaranteed return claims
- Neutral interface design avoiding dark patterns or manipulative UX
- Standardized risk ratings and consistent disclosure presentation

These accountability mechanisms have been implemented through platform design, smart contract architecture, and comprehensive disclosure without requiring traditional registration frameworks that assume custody or discretionary management.

Proposed Framework: Conditional Safe Harbor for Non-Custodial Applications

We propose the Commission consider a narrow, conditional safe harbor that would provide regulatory clarity for non-custodial onchain applications that meet specific criteria:

Qualifying Conditions

To qualify for safe harbor treatment, a platform must:

1. Never hold, custody, or control user assets

- No private keys, seed phrases, or signing authority over user funds
- No pooled accounts or omnibus structures
- No ability to unilaterally move, freeze, or access user funds
- Smart account infrastructure maintains user as ultimate controller

2. *Not execute transactions on users' behalf*
   - All transactions signed and broadcast by users directly from their wallets
   - No discretionary trading, portfolio management, or rebalancing without explicit user-initiated action
   - No authority to act without user signature for each transaction
   - Automated strategies execute only based on pre-defined, user-selected parameters

3. *Provide standardized risk and protocol disclosures*
   - Smart contract audit status, audit firm identity, and date of most recent audit
   - Protocol risk factors (smart contract risk, economic risk, operational risk)
   - Historical performance data with appropriate disclaimers and context
   - Clear statements that past performance does not predict future results
   - Validator attestation status and bonding levels

4. *Maintain clear conflict-of-interest disclosures*
   - All economic relationships with listed protocols and vault strategies
   - Complete fee structures including protocol fees, platform fees, and execution costs
   - Affiliated vs. third-party protocol distinctions
   - Revenue models and any marketing or promotional arrangements
   - Validator and strategist staking/bonding disclosures

5. *Avoid dark patterns and maintain neutral interface design*
   - No manipulative design elements or pressure tactics
   - No misleading yield projections, guarantees, or "risk-free" representations
   - Balanced presentation of risks alongside potential opportunities
   - User control over information display, filtering, and comparison tools
   - Clear cancellation and exit procedures with no hidden lock-ups

6. *Publish operator transparency and governance information*
   - Entity structure, jurisdiction, and regulatory status
   - Team information and relevant background
   - Contact information, customer support channels, and dispute resolution procedures
   - Governance structure and token holder rights (if applicable)
   - Clear explanation of emergency procedures and circuit breaker mechanisms

Safe Harbor Benefits

Platforms meeting these conditions would receive clarity that:

- They are not broker-dealers under the Exchange Act
- They are not investment advisers under the Advisers Act
- They are not operating investment companies under the Investment Company Act
- Their facilitation of user access to DeFi protocols does not constitute securities "offers" or "sales"

- Compliance focus shifts to disclosure, transparency, and user protection standards rather than custody-based frameworks

This framework would enable continued innovation in user experience and financial infrastructure while ensuring meaningful user protection through disclosure, auditing, and transparency rather than through regulatory frameworks designed for fundamentally different business models.

Section 230 as Precedent for Platform Liability Principles

The Communications Decency Act's Section 230 provides instructive precedent for how platforms can facilitate user access to third-party services without bearing liability for user choices. Key parallels:

Platform vs. Publisher Distinction

- Section 230 distinguishes platforms providing access from publishers creating or controlling content
- Similarly, non-custodial aggregators provide access and information about DeFi protocols but don't manage assets or make investment decisions
- Users make independent choices about which protocols to interact with based on disclosed information
- Platform's role is facilitation and information aggregation, not recommendation or discretionary management

No Liability for Third-Party Actions

- Under Section 230, platforms aren't liable for third-party content or user actions absent platform's own illegal conduct
- Analogously, non-custodial platforms shouldn't be liable for user investment choices or outcomes of third-party protocols
- Platform's obligation is accurate disclosure about third-party protocols, not guarantees of protocol performance
- Distinction recognizes that users are sophisticated enough to make their own decisions with proper information

Good Samaritan Provisions

- Section 230(c)(2) protects voluntary content moderation efforts
- Parallel principle: aggregators that screen for obvious scams, require audits, or provide risk ratings shouldn't face increased liability for curation efforts
- Encouraging responsible platform design and user protection without creating perverse incentives
- Platforms should be rewarded, not penalized, for implementing security standards beyond minimum requirements

Limits and Boundaries

- Section 230 doesn't protect platforms' own illegal conduct or intellectual property violations
- Similarly, proposed safe harbor wouldn't shield fraud, market manipulation, misrepresentation, or violations of other laws
- Platforms remain subject to anti-fraud provisions (Securities Act Section 17(a), Exchange Act Section 10(b) and Rule 10b-5)
- Distinction is between liability for facilitating access vs. liability for platform's own conduct

The Section 230 analogy demonstrates how regulation can appropriately distinguish between:

- Platforms that provide access, information, and tools (disclosure-focused regulatory approach)
- Platforms that exercise control, custody, and discretion (fuller custody-based regulatory framework)

This same principle should apply to non-custodial onchain applications: accountability through disclosure, security standards, and transparent design rather than through regulatory frameworks that assume intermediation and control.

[Superform's Technical Implementation of User Protection Standards]

Superform has invested significant financial, engineering, and security resources in implementing comprehensive user protection mechanisms that could inform industry-wide standards:

Smart Contract Security and Auditing

- Multiple comprehensive audits by leading firms (yAudit, Spearbit with multiple independent researchers)
- Continuous monitoring for anomalies, exploits, and protocol risks
- Vault simulation system tests deposits and withdrawals before users commit funds
- Automatic alerts and de-listing protocols for security events or anomalous behavior
- User-facing security scoring and audit status display for all listed vaults

Transaction Transparency and Auditability

- All routing logic, fees, and strategy execution is on-chain and publicly auditable
- Users can verify exact assets, amounts, destinations, and fees before signing transactions
- Complete transaction history and audit trail accessible to users
- No hidden fees, opaque execution, or undisclosed revenue streams

Risk Communication and User Interface Standards

- Standardized risk taxonomy and visual hierarchy across all vault types
- Prominent display of audit status, validator attestations, and security indicators
- Educational resources explaining DeFi concepts, risks, and technical requirements
- Jurisdiction-based content restrictions and compliance controls
- Clear disclaimers on yield volatility and principal risk

User Control and Self-Custody Preservation

- Users can interact with underlying protocols directly at any time, bypassing Superform if desired
- No lock-ups, withdrawal restrictions, or permission requirements imposed by Superform platform
- Emergency withdrawal capabilities preserved regardless of platform status
- Full self-custody maintained throughout entire user journey via smart account architecture
- Users can migrate assets and strategy positions without Superform involvement

These technical implementations demonstrate how meaningful user protection can be achieved through transparent design, rigorous security practices, and disclosure-focused standards rather than through traditional custody-based regulation. Superform would welcome the opportunity to provide detailed technical documentation and demonstrations to inform Commission thinking on appropriate standards.