MEMORANDUM

To:	Crypto Task Force Meeting Log
From:	Crypto Task Force Staff
Re:	Meeting with a Representative of CompliLedger

On January 20, 2026, Crypto Task Force Staff met with a representative from CompliLedger.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. The CompliLedger representative provided the attached documents, which were discussed during the meeting.

Proposed Meeting Agenda – SEC Crypto Task Force
Focus: Regulation S-P, Regulation S-ID, Cybersecurity Safeguards, Recordkeeping

Proposed Duration: 45–60 minutes

1. Introduction and Regulatory Context (5–10 min)
Overview of regulatory drivers, including Reg S-P safeguarding requirements, Reg S-ID identity theft prevention, cybersecurity risk management expectations, and recordkeeping obligations applicable to SEC-regulated entities.

2. Operationalizing Regulation S-P Safeguards (10–15 min)
Discussion of how firms translate safeguarding and data minimization requirements into technical and organizational controls, including monitoring, access controls, and vendor risk considerations.

3. Regulation S-ID and Identity Theft Prevention (10–15 min)
Exploration of challenges implementing red flags programs in technology-driven environments, maintaining auditability, and ensuring programs evolve with emerging threat patterns.

4. Cybersecurity Safeguards and Evidence Generation (10–15 min)
Discussion of continuous versus point-in-time cybersecurity compliance, alignment of policies with technical enforcement, and generation of defensible evidence for supervisory review.

5. Recordkeeping, Auditability, and Supervisory Transparency (10–15 min)
Consideration of record accuracy, integrity, retention, and accessibility, and how standardized compliance artifacts may support regulatory oversight while preserving intent.

6. Closing Discussion and Staff Feedback (5–10 min)
Open discussion on observed industry risks, compliance tooling guardrails, and constructive engagement between regulators and compliance technology providers.

Proposed Attendees – SEC Crypto Task Force Meeting

Requesting Participant
Maranda Harris
Founder & Chief Compliance Officer, CompliLedger

Requested SEC Participants (as available and appropriate)
Veronica Reynolds – SEC Crypto Task Force
Sumeera Younis – SEC Crypto Task Force / Policy
Donald Battle – SEC (Policy / Regulatory Affairs)
Landon Zinda – SEC (Cybersecurity, Risk, or Technology Policy)
Representative from the Division of Examinations (policy, risk, or cybersecurity advisory role)

Additional SEC participants are welcome at staff discretion based on subject-matter relevance.

Compliance Automation in Digital Asset Markets – Discussion Brief

Purpose of This Brief

This document is provided to support an informational discussion with the SEC Crypto Task Force regarding emerging compliance automation practices used by digital asset and technology-driven financial firms. The purpose is not to seek legal advice, interpretive guidance, or regulatory relief, but to facilitate dialogue on supervisory expectations, implementation considerations, and potential risks as compliance tooling evolves.

Regulatory Context

Digital asset firms increasingly fall within the scope of SEC requirements related to customer information protection, identity theft prevention, cybersecurity governance, and recordkeeping. Key regulatory drivers include:

- Regulation S-P safeguarding and privacy obligations
- Regulation S-ID identity theft red flags programs
- SEC cybersecurity risk management and incident preparedness expectations
- Recordkeeping and supervisory transparency requirements

As these requirements expand in scope and enforcement focus, firms are increasingly turning to automated compliance tooling to operationalize obligations that were historically managed through manual or point-in-time processes.

Observed Industry Challenges

Across industry, several recurring challenges have emerged:

- Translating regulatory text into consistently enforced technical controls
- Aligning written policies with real-world system behavior
- Demonstrating ongoing compliance rather than static compliance snapshots
- Balancing regulatory transparency with protection of sensitive or proprietary data

Compliance Automation Considerations

Compliance automation tools can offer meaningful benefits, including improved consistency, audit readiness, and reduced operational burden. However, they also introduce risks if not properly governed. Key considerations include:

- Ensuring automation supports, rather than replaces, human judgment and accountability
- Maintaining transparency and auditability of automated processes
- Avoiding “checkbox compliance” that obscures substantive control effectiveness
- Ensuring records generated through automation remain accurate, complete, and reviewable

Privacy, Data Minimization, and Evidence Generation

A central challenge for firms is demonstrating compliance with safeguarding, cybersecurity, and recordkeeping obligations without unnecessary over-disclosure of sensitive data. Emerging approaches emphasize:

- Data minimization and least-privilege access principles
- Evidence generation that demonstrates control effectiveness without exposing underlying customer data
- Clear governance over how compliance artifacts are created, retained, and reviewed

Discussion Objectives

This meeting seeks SEC staff perspectives on:

- Common deficiencies or risks observed in compliance automation approaches
- Guardrails technology providers should consider to preserve regulatory intent
- Areas where further clarity or industry engagement may be beneficial

This dialogue is intended to support responsible innovation while reinforcing investor protection, market integrity, and effective supervisory oversight.