Reimagining Compliance, and KYC / AML: Better Ways to Catch Bad Actors

June 13, 2025 | Dirksen Senate Office Building

Co-Chairs: Michelle O'Connor, Taxbit; Shih Yun Chia, VerifyVASP

1. The Nature of Bad Actors and Evolving Threats

- Decentralized and sophisticated: Bad actors operate globally with professional-grade operations, mirroring the capabilities of modern tools (e.g. AI).
- Cybercrime is primary, not just a digital version of traditional crime.
- Jurisdictional fragmentation complicates enforcement (e.g. OFAC vs China lists).
- Supply chain-level granularity: Organized crime has infiltrated entire systems, not isolated points.
- Existing safeguards are inadequate and reactive, not preventative.

2. Limitations of Current Compliance Structures

- Traditional financial crime is no longer the central concern for compliance. Misinformation, disinformation, and even climate-linked externalities are creeping into the scope.
- Typology-focused risk assessments are outdated. Behavioral and contextual models are needed.
- Suspicious Activity Reports (SARs) have been misapplied; they were meant to surface behaviour, not to solve crimes.
- Compliance often lacks nuance, lumping together:
    - Criminal laundering
    - Regulatory non-compliance
    - Market manipulation (e.g. meme coins, pump-and-dump)
    - Informal but non-illicit behavior
- This contributes to exclusion of legitimate users from financial systems.

3. Systemic & Structural Issues

- Compliance is often a "copy-paste" from TradFi models ill-suited for decentralized systems.
- Tools intended for inclusion (e.g. blockchain) often replicate exclusion.
- The regulatory focus is misaligned regulators expect to see known patterns, not emerging behaviours.
- Regulatory perimeter is tightening, driven by FATF Recommendations 10, 15, 16 and Travel Rule enforcement.
- Greylisting and mutual evaluations are influencing regulatory aggression, especially toward VASPs.
- Current models favor the well-funded and centralized actors; smaller players are penalized by overhead.

4. Digital Identity & Data Handling

- Digital identity should be modular (boolean attributes) not monolithic.
- Real-world examples highlight inefficiencies:
    - Singapore: Over-collection via digital onboarding.
    - USA: Manual, in-branch processes still dominate.
- Data permissioning can allow PII to be used without overexposure.
- In a DeFi context, KYC obligations are unclear and peer-to-peer interactions blur responsibility.

5. Governance & Community

- Governance in a decentralized identity system remains unresolved.
- There's power in industry collaboration, even if informal:

    - The ByBit example demonstrates community-led risk flagging.
- SARs are siloed, even though sharing them could dramatically improve detection and prevention.

6. Technology: Opportunity vs Risk

- AI codifies existing biases unless consciously addressed.
- Introduces concentration risk, especially in compliance tooling.
- 'Six hops' rules and transaction tracing lack context and may produce false risk flags.
- Emphasis on human-in-the-loop systems to apply judgment and context.

7. Reframing Compliance

- We need to flip compliance models:
    - Focus on enabling safe participation, not only blocking risk.
    - Embed tooling that addresses distinct risk categories individually.
    - Reframe compliance from punitive to enabling support innovation while safeguarding integrity.

Suggestion: Industry-led regulation drafting, demonstrating what works, not waiting for prescriptive frameworks.