

Shield Client Connect 2026

Opening Address Summary | For Shield Team Review

Leading during times of uncertainty

In my opening address, I argued that responsible cannabis banking is a test of leadership. Financial institutions should not ignore risk, but neither should they treat complexity as an automatic reason to walk away. The question I asked is whether an institution can understand the risks, put the right controls in place, and serve customers responsibly.

My central point was simple: high risk is not the same as unacceptable risk. We must make informed decisions within a clear risk appetite—and build the knowledge, controls, and governance needed to support them.

Why I believe this matters

I connected my advocacy for hemp in Kentucky and my later work on cannabis banking as NCUA Chairman to a consistent principle: lawful businesses should have a fair opportunity to access financial services, and financial institutions must meet that opportunity with strong compliance. I view this as a matter of financial inclusion, public safety, transparency, and responsible service—not as an argument for relaxing standards.

I emphasized that when legitimate businesses are shut out of the banking system, their financial activity does not disappear. It can become more cash-dependent and less transparent. Well-governed financial relationships can support safer payments, payroll, tax remittances, stronger records, and greater accountability.

The market is substantial, but access remains incomplete. Shield's 2026 survey found that operators were generally satisfied with their banking relationships while commercial credit remained difficult to obtain. Federal policy is evolving, but rescheduling does not itself legalize cannabis or create a banking safe harbor, and the SAFE Banking Act remains pending legislation. Institutions must continue to follow applicable law and guidance.

Institutions showing leadership

I recognized institutions that have moved beyond a wait-and-see posture: Needham Bank's expanded Curaleaf credit facility; Valley Bank's specialized cannabis program; Salal Credit Union's long-running service and expansion; Dart Bank's significant cannabis and hemp customer base; and Union Bank's move from deposits into lending. Their approaches differ, but each illustrates the value of building expertise and controls around a complex market.

My action agenda for financial institutions

1. Make a deliberate strategic decision.

I urged institutions to prepare a written assessment for the board that explains the community or member need, strategic fit, target customers, expected economics, legal considerations, reputational implications, and operational requirements. We should distinguish the decision to learn about the market from the decision to enter it. We should document why the activity fits—or does not fit—the institution's charter, field of membership, resources, and risk appetite.

2. Set clear boundaries before onboarding customers.

I urged boards and management teams to define eligible and ineligible customers, business activities, products, and jurisdictions; identify prohibited activity; and establish limits for customer and sector concentration, cash exposure, lending, and vendor dependence. Institutions should decide who may approve exceptions, how exceptions will be reported, and what circumstances call for escalation, remediation, restriction, or exit.

3. Check operational readiness.

Before launch, map the full customer and transaction lifecycle—from referral and onboarding through monitoring, lending, audit, and account closure. Assess whether staffing, expertise, data, technology, legal support, vendor capacity, and audit resources are sufficient. Test whether the institution can identify related entities, verify license status, monitor expected activity, aggregate exposure, and give the board useful reports. Assign an owner and deadline to every readiness gap.

4. Build due diligence around the customer's actual business.

I called for a consistent process to understand the entity, beneficial owners, control persons, licenses, locations, business model, related companies, expected transaction activity, counterparties, source of funds, and relevant regulatory history. Verify important information where possible rather than relying only on customer attestations or vendor outputs. Refresh due diligence when ownership, licensing, locations, management, or business activity changes.

5. Make ongoing monitoring meaningful.

Translate what we know about each customer into a reasonable picture of expected activity, including deposits, payments, payroll, taxes, vendors, transfers, and cash use. Set monitoring rules that reflect the customer's business and risk. Establish clear procedures for investigating alerts, documenting decisions, escalating concerns, making SAR decisions, and reviewing case quality. Keep the SAR decision distinct from the decision to retain, restrict, remediate, or exit the relationship, while ensuring those decisions are coordinated and documented.

6. Manage cash, payments, and day-to-day operations.

Document how cash is generated, counted, transported, deposited, reconciled, and safeguarded. Understand payment flows, the parties involved, and the business purpose of transactions. Establish procedures for unusual cash patterns, unexplained third-party activity, transactions inconsistent with expected business, fraud, cybersecurity incidents, and operational disruptions.

7. Treat lending as a separate capability.

A deposit relationship does not automatically establish creditworthiness. Create separate underwriting standards for working capital, equipment, real estate, and other products. Assess repayment capacity, collateral and lien enforceability, licensing and legal contingencies, concentration, market volatility, covenants, stress scenarios, and workout options. Pilot carefully, review performance, and expand only when the data and controls support it.

8. Oversee vendors and technology.

Identify every third party supporting onboarding, license checks, monitoring, payments, cash logistics, data, or customer service. Review its expertise, cybersecurity, continuity planning, subcontractors, and concentration risk. Contracts should provide appropriate access to data, audit rights, incident reporting, regulatory cooperation, and transition or termination assistance. Maintain enough internal expertise to question vendor outputs; technology can assist judgment, but it cannot replace it.

9. Train employees and support independent challenge.

Provide role-specific training on onboarding, red flags, escalation, documentation, cash handling, and individual responsibilities. Give the BSA officer and risk and compliance teams the authority, information, staffing, and access to senior leadership needed to do their jobs. Use practical exercises—a license suspension, unusual activity, cash discrepancy, vendor outage, or legal change—to test readiness and capture lessons.

10. Measure performance and report candidly.

Give management and the board a clear view of customer and sector exposure, concentrations, transaction and cash trends, alert volumes and aging, SAR decisions, exceptions, complaints, license changes, audit findings, vendor issues, and overdue remediation. Independent testing should assess whether controls work in practice, not just whether policies exist. Escalate recurring issues and growth that outpaces staffing or control capacity.

11. Maintain open supervisory and policy dialogue.

Communicate with supervisors about strategy, program boundaries, controls, material issues, and significant changes. Keep a clear record of the institution's rationale and decisions. Share practical experience with policymakers on compliance workload, payment access, credit availability, customer impacts, and the effects of uncertainty—without overstating what proposed laws or policy directives have changed.

12. Prepare for change, but do not assume it.

Assign responsibility for tracking legislation, agency guidance, rescheduling, and other legal developments. For each change, determine what it actually does, who it affects, and whether procedures must change. Until the law or applicable guidance changes, continue to meet current obligations. Apply the same disciplined approach to digital assets, tokenized deposits, artificial intelligence, faster payments, and fintech partnerships.

Closing thought

I challenged institutions to replace reflexive avoidance with informed judgment. Build the knowledge. Build the controls. Build the trust. Then use those capabilities to serve legitimate customers and help shape the future of financial services.

This summary is for conference and strategic discussion, not legal advice. Institutions should confirm current requirements with qualified legal and compliance professionals.