From Pilot to Production: How Banks and Payments Companies Launch Stablecoin Services

October 23, 2025

Christopher L. Boone
Partner | +1 202.344.4248 | clboone@Venable.com

VENABLE LLP

Agenda

- Landscape and legal anchors for payment stablecoins
- Program architectures and end-to-end payment flows
- Financial crimes compliance and sanctions readiness
- Consumer protection and truthful marketing practices
- Third-party risk management, from planning to exit
- Summary Cheat Sheet and evidencing compliance

VENABLE LLP

Why Stablecoins, Why Now?

- Stablecoins are moving from proofs of concept to live payment programs because they promise faster settlement and programmable features.
- A federal framework now defines who may issue payment stablecoins and what consumer and safety obligations they must meet.
- Banks and payment companies can participate if they operate with bank-grade risk management and documented evidence of control effectiveness.
- **Core appeal:** Stablecoins combine the efficiency, programmability, and global reach of blockchain with price stability that traditional crypto lacks.
- **Primary use cases:** Payments (especially cross-border), remittances, merchant settlement, DeFi collateral, treasury management, and digital dollar access in high-inflation regions.

VENABLE LLP

Definitions and Players

- A **payment stablecoin** is a digital representation of value that is designed to maintain a stable price and to be used for payments, with reserves that are held in high-quality assets.
- A **digital asset service provider** (DASP) is a company that operates wallets, exchange functions, or transfer services for digital assets.
- A **custodian** safeguards reserve assets or cryptographic keys and is responsible for segregation, reconciliation, and resiliency.

VENABLE LLP

How Fiat-Backed Stablecoins Work

- **Minting and redemption**: Users deposit fiat (e.g., USD) with the issuer; the issuer mints an equivalent amount of tokens (e.g., USDC) and sends them to the user's blockchain wallet. Redemption works in reverse, tokens are burned, and fiat is transferred back.
- **Reserve model**: Reserves are held in cash or near-cash instruments (e.g., Treasury bills). Reputable issuers provide audits or daily disclosures, and/or operate through regulated funds (e.g., SEC-registered money market funds).
- **Programmability and interoperability**: Stablecoins can work across compatible wallets, blockchains, and DeFi protocols, enabling automated payments, escrow, yield distribution, and seamless cross-platform use.

VENABLE LLP

The Regulatory Landscape

VENABLE LLP

Legal Anchor: GENIUS Act

- Signed into law on July 18, 2025.
- The GENIUS Act marks a milestone in digital-asset regulation, creating a federally approved regulatory framework for U.S. dollar-backed stablecoins.
- Banks, payment companies, and issuers must prepare for significant changes in the regulatory landscape.
- Set to take effect by the earlier of 18 months from enactment or 120 days after the primary federal stablecoin regulators issue rules implementing the act.

VENABLE LLP

GENIUS Act: Key Takeaways

- **Licensing Required:** All U.S. stablecoin issuers must register as Permitted Payment Stablecoin Issuers (PPSIs).
  - Eligible issuers: banks, nonbank companies (via OCC charter), or state-licensed firms (if state regime meets standards)
  - "Shot Clock" for Application Decisions
- **1:1 Reserves and Redemption Guarantee**
  - Backing required: cash, Treasuries, insured bank deposits, etc.
  - Reserves must be segregated, audited, and bankruptcy-protected.
- **Ban on Interest-Bearing Stablecoins**
  - Stablecoins cannot offer yield or function as investment product.
- **Regulatory Oversight Split by Size**
  - $10B in circulation → mandatory federal oversight.
  - Less than $10B → may operate under certified state regimes.

VENABLE LLP

GENIUS Act: Guardrails

- **Prohibits Unlicensed Stablecoins in U.S. after 3-Year Transition**
  - U.S.-based platforms barred from supporting “non-compliant” coins.
  - Treasury may approve reciprocal foreign regimes for offshore stablecoins.
- **Priority Claim in Bankruptcy**
  - Stablecoin holders get first access to reserves in insolvency.
- **Monthly Attestations and Public Disclosures**
  - Reserve reports must be independently reviewed and signed by CEO/CFO.
- **Prohibits Rehypothecation of Reserves**
  - Reserves can’t be pledged or reused—held purely for redemptions.
- **Custody Rules Override SEC SAB 121**
  - Bars regulators from forcing custodians to treat stablecoin assets as liabilities.

VENABLE LLP

Digital Asset Service Providers (DASPs)

- Three years after enactment, DASPs may offer or sell payment stablecoins in the U.S. **only if** the stablecoins are issued by a permitted issuer (or by foreign issuers meeting equivalence standards).
- **DASPs are business that:**
  - (1) are compensated for exchanging digital assets for money or other digital assets;
  - (2) transfer digital assets to a third party;
  - (3) act as custodian of digital assets; or
  - (4) are participating in financial services relating to digital asset issuance.
    - Excludes: Entities that develop a distributed ledger protocol, operate a distributed ledger, validate transactions, or participate in a pool providing liquidity for peer-to-peer transactions.
  - With certain exceptions, custodians must maintain separate accounting for payment stablecoins and reserves, which cannot be commingled with other assets.

VENABLE LLP

Building a Program

VENABLE LLP

Common Program Structures

- **Architecture A: Bank-issued token**
  - The bank issues the token and controls minting and burning through bank-governed signers.
  - Reserve assets sit within the banking perimeter and are reconciled daily.
- **Architecture B: Nonbank issuer with bank partners**
  - A nonbank issuer qualifies under an applicable pathway and partners with banks for reserve custody and fiat rails.
- **Architecture C: Service provider using a permitted issuer's token**
  - A third party integrates a permitted issuer's token and provides wallets, checkout, or settlement tools.
- Contracts assign responsibilities for identity verification, sanctions screening, wallet analytics, and customer servicing.

VENABLE LLP

Program Scoping

- Determine precisely who you are in the ecosystem and the outcome you are trying to deliver, such as accepting card payments for token purchases, enabling payouts in stablecoins, or providing custody.
- Identify every third party needed to execute the services, specify what each will do, and document those assignments in a responsibility matrix covering the issuer, payment intermediaries, digital asset service providers, custodians, and any other service providers.
- For each function, onboarding, funding, token issuance, transfers, redemption, treasury, technology operations, and support, name the single accountable owner.
- Set measurable service levels that matter to customers and partners.

VENABLE LLP

Flow of Funds and Control Points

- Draw a single end-to-end picture that traces money and tokens from funding through redemption. Identify the direction of movement and the handoff between systems so there is no ambiguity about where value resides at each moment.
- Funds moving into the system trigger token issuance with reconciliation of cash, tokens minted, and reserves held.
- Redemption and funds moving out of the system follow service-level timelines, exception handling, and error-resolution procedures.
- Issuance/redemptions are subject to transaction screening, anomaly detection, and documented controls and overrides.
- Daily position reconciliations align tokens outstanding, reserve statements, and treasury balances.
- Reserve assets are held in segregated accounts with restricted use.

VENABLE LLP

Working with DASPs or Integrating Stablecoin Services

- Confirm lawful purpose and regulatory compliance
- Verify ownership and leadership integrity
- Validate business model and map the full flow of funds
- Review consumer terms and marketing
- Assess financial condition and protections
- Evaluate fraud prevention and dispute handling
- Examine third-party dependencies
- Check operational readiness and service levels

VENABLE LLP

Program Compliance

VENABLE LLP

What Regulators Expect:
Industry Standards and Supervision

Supervisory Expectations

- **Risk Management Frameworks**: Issuers and DASPs must integrate crypto activities into their enterprise-wide risk management, audit, and compliance programs. This means crypto activities should not be siloed or treated as exceptions.
- **Technology and Expertise**: Supervisors expect issuers and DASPs to build or access sufficient expertise to manage blockchain-related risks, rather than simply relying on vendors.
- **Ongoing Examination Focus Areas**:
  - Risk governance, including board oversight of crypto activities
  - Internal controls and audit trails for crypto transactions
  - Compliance with evolving regulatory guidance (OCC, FDIC, Fed, FinCEN, SEC)

VENABLE LLP

What Regulators Expect:
Controls in Production

- **Safety and Soundness:** Issuers and DASPs must ensure crypto activities do not jeopardize capital, liquidity, or operational resilience, including maintaining and safeguarding appropriate liquidity buffers (e.g., for stablecoin reserves) and balancing operation risks (e.g., prudent balance sheet exposure).
- **Monitoring and Testing:** Full compliance with Bank Secrecy Act (BSA), anti-money laundering (AML), and sanctions laws applies. Issuers and DASPs must implement crypto-specific transaction monitoring, customer due diligence, and suspicious activity reporting.
- **Third-Party Risk Management (TPRM):** Issuers and DASPs using fintechs or vendors for custody, payments, or execution must follow robust TPRM frameworks (e.g., OCC Bulletin 2023-15), including vendor diligence, contractual safeguards, and oversight.

VENABLE LLP

What Regulators Expect:
Controls in Production (cont.)

- **Operational and Cybersecurity:** Regulators expect issuers and DASPs to demonstrate adequate blockchain transaction expertise and controls against cyber threats unique to crypto environments (e.g., private key theft, smart contract exploits).
- **Consumer Disclosures:** Issuers and DASPs must ensure and prioritize transparency, including fee structures and redemption rights and using plain language requirements.
- **Retention Policies:** Entities must implement formal retention policies to preserve communications and records.

VENABLE LLP

Money Transmission and Financial Crimes Compliance

- A party that accepts and transmits (or exchanges) value is generally treated as a money transmitter and must register as a money-services business (MSB).
  - A nonbank that issues a stablecoin is generally a money transmitter because it accepts and transmits value.
  - Banks are not considered MSBs but remain subject to Bank Secrecy Act compliance obligations.
  - Custodians and many DASPs will also fall under money transmissions rules.
- **The GENIUS Act states that a stablecoin issuer is treated as a "financial institution" for Bank Secrecy Act purposes.**
  - The statute directs FinCEN to set tailored anti-money-laundering and sanctions standards for these issuers.
  - Until tailored rules are fully implemented, nonbank issuers should assume the existing money-transmitter obligations continue to apply.

VENABLE LLP

AML Compliance Program Pillars

- A risk-based program includes customer identification, sanctions screening, monitoring, investigations, recordkeeping, and reporting.
- **Internal Controls:** Policies, procedures, and internal controls to ensure ongoing AML compliance
- **Independent Testing:** Internal independent testing, or external audits, to monitor program for compliance
- **Officer:** Designation of an AML compliance officer
- **Training:** Provided for appropriate personnel
- **Risk-Based CDD/KYC Program:** A risk-based approach to customer due diligence (CDD) and ongoing monitoring

VENABLE LLP

Customer Identification Program (for Banks)

- The CIP rule requires banks to obtain information sufficient to form a reasonable belief regarding the identity of each customer opening a new account.
- At minimum, the following info must be obtained:
  - Name
  - Date of birth, for an individual
  - Address
  - Identification number
- The CIP must contain procedures for verifying the identity of the customer using the information obtained as outlined above (through documents and through non-documentary methods).

VENABLE LLP

OFAC and Sanctions Basics

- U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is responsible for overseeing and enforcing economic sanctions.
- Who must comply with U.S. sanctions?
  - All U.S. persons, generally defined to cover the following:
    - U.S. citizens and lawful permanent residents, regardless of location;
    - persons and entities within the United States, regardless of nationality; and
    - U.S.-incorporated entities, including their foreign branches.
- Certain OFAC programs also apply to certain non-U.S. persons, such as foreign persons in possession of U.S. goods, and foreign subsidiaries who happen to be owned or controlled by a U.S.-based company can find themselves subject to U.S. sanctions programs.
- Non-compliance can mean significant criminal and civil penalties, including on a strict-liability basis—meaning that an organization can be liable even without knowledge of the violation being committed.

VENABLE LLP

Consumer Protection and Truthful Marketing

- Disclosures explain reserve backing, redemption rights, limitations, and how value may fluctuate during abnormal market conditions.
- No statement implies deposit insurance or guaranteed value beyond what the program can actually deliver.
- Complaint handling, refunds, and error resolution follow written policies and partner obligations, and the program measures and reports performance.
- Marketing claims are pre-cleared through legal and compliance, substantiated with evidence, and consistent across the website, app stores, and social media; endorsements follow Federal Trade Commission rules, and no bank logos or “insured” language appears unless it is strictly accurate.

VENABLE LLP

Redemption Policy and Service Levels

- **Must publicly post a redemption policy**
  - State redemption at par, receipt methods, cutoff times, and dispute handling in plain language.
  - Operations should test redemption timelines through regular testing and record actual performance against the stated standards.
  - Exceptions are tracked, resolved, and reported to governance bodies with root-cause analysis.

VENABLE LLP

Third-party Risk Management (TPRM)

- Third-party risk management is the set of governance, risk, and control activities a financial institution uses to identify, assess, contract for, oversee, and exit relationships with external service providers across the full life cycle, including planning, due diligence, contracting, ongoing monitoring, and termination.
- Vendor management is the operational discipline that applies these life-cycle controls to specific service providers, including technology outsourcers, wallet and key-management firms, analytics vendors, custodians, and compliance utilities.
- Banking supervisors and the Federal Financial Institutions Examination Council (FFIEC) provide detailed expectations for outsourced technology services.
- Nonbank financial institutions are also expected to oversee service providers.

VENABLE LLP

Third-party Risk Management – Critically Important

- Stablecoin programs depend on chains of counterparties, including issuers, reserve custodians, wallet operators, blockchain infrastructure providers, and analytics firms, so operational and compliance failures at any one provider can disrupt minting, burning, redemption, or consumer support.
    - Interagency guidance highlights that risk and criticality vary by relationship and require a risk-based program.
- Stablecoin use introduces cybersecurity risk, including key custody, signing services, smart-contract upgrades, and node or validator operations, which must be governed within the organization's broader enterprise risk management and cybersecurity strategy.
    - The Cybersecurity Framework version 2.0 expressly integrates third-party and supply-chain risk into governance expectations.

VENABLE LLP

Third-party Risk Management – Program Elements

- **Governance and risk appetite:** The board or senior leadership approves a written framework that defines roles, decision rights, risk appetite, and escalation paths for partners that support minting, custody, wallet operations, and incident response.
- **Pre-contract due diligence:** The organization evaluates financial condition, regulatory posture, compliance history, leadership competence, information security, operational resilience, and subcontractor chains.
- **Contracting and controls:** Agreements assign responsibilities, audit and data rights, service-level targets, and exit and transition assistance.
- **Ongoing monitoring and testing:** Ongoing monitoring is tailored to the third party's responsibilities, the criticality of the service, and the potential impact on customers, reserves, or redemption.
- **Exit strategy and resilience:** The organization maintains playbooks for rapid termination or replacement, including data return, key transfer, consumer communications, and continuity of services.

VENABLE LLP

Balancing Innovation with Industry Realities

Industry Realities

- **Crypto activities are still seen as novel**: Even as barriers drop, regulators remain cautious and will scrutinize activities through standard safety, soundness, and compliance lenses.
- **Regulatory guidance is evolving**: Joint agency guidance is expected to provide clearer guardrails; until then, issuers and DASPs are held to high internal governance standards.
- **Increase in crypto adoption:** Crypto is experiencing significant mainstream adoption by retail consumers and institutions. With this growth comes the need to balance innovation with regulatory compliance and safety controls.

VENABLE LLP

Summary Cheat Sheet – Practical Steps

Translating Requirements into Program Artifacts

- Implement and codify company policies proactively and diligently address regulator expectations.
- Routinely conduct testing and maintain testing records.
- Ensure compliance and legal team involvement in product and service development from inception through launch and maintenance.

Evidencing Compliance to Regulators and Counterparties

- Attestations of training attendance and understanding
- Targeted training modules for finance, product, and customer-facing teams
- Routine independent audits or testing made available to regulators

VENABLE LLP

Concluding Thoughts

VENABLE LLP

Questions?

Christopher L. Boone
Partner
+1 202.344.4248
clboone@Venable.com

Chris Boone helps clients navigate the regulatory environments that govern payment processing and provides counsel on all manner of agreements, including merchant processing and sponsorship. He works with banks, processors, independent sales organizations (ISOs), payment facilitators, merchants, and fintech businesses to address the legal, operational, and business challenges of payment and transaction processing, including payment structures and forms of mobile and digital payments. A cornerstone of Chris's practice focuses on regulatory compliance issues related to cryptocurrencies, token platforms, and NFTs. Chris is regularly sought out for his robust technical knowledge of blockchain systems and his experience with emerging legal issues in the cryptocurrency space.

VENABLE LLP

VENABLE LLP