THE GENIUS ACT IN 2026

BY THOMAS GRUNDY, CRCM

A strategic inflection point for U.S. banks

WHEN CONGRESS ENACTED the Guiding and Establishing National Innovation for U.S. Stablecoins Act, commonly referred to as the GENIUS Act (the Act), it did more than establish the first federal framework for payment stablecoins, it signaled a structural shift in U.S. financial infrastructure, moving digital asset payments from the periphery of experimentation to the center of regulatory and strategic focus. By 2026, that shift becomes operationally unavoidable for banks as rulemaking is accelerating, competitive boundaries are being redrawn, and the decisions institutions make now will determine their relevance in the next generation of payments.

Stablecoins have matured into mainstream liquidity tools powering global platforms, and the Act brings them squarely into the regulated perimeter as a new class of payment instrument. For banks, this moment is both challenge and opportunity, introducing new supervisory expectations while opening the door to new revenue models, customer segments, and roles in the digital asset ecosystem. Institutions that move decisively will shape the market; those that hesitate will find themselves navigating a landscape defined by others.

The rulemaking process: Where the Act implementation stands in 2026

The Act's one-year implementation deadline has driven an unusually accelerated regulatory cycle, pushing federal banking agencies from conceptual frameworks to fully formed rule proposals in record time. By early 2026, the regulatory perimeter for payment stablecoins is no longer theoretical as agencies are constructing a prudential regime designed to prevent runs, protect consumers, and impose transparency on a market that has historically operated outside traditional oversight. As these rulemakings advance in parallel, the industry is entering a defining moment. The Act is not merely a compliance mandate; it is the foundation of a new payments architecture in which digital dollars are expected to operate with the same safety, stability, and supervisory discipline as established financial instruments.

The Office of the Comptroller of the Currency (OCC) has led the way and continues to set the tone for the broader regulatory landscape. On February 25, 2026, the OCC issued a sweeping 350-plus-page Notice of Proposed Rulemaking (NPR) that addresses nearly all prudential requirements under the Act.[1] The proposal establishes uniform standards for becoming a Permitted Payment Stablecoin Issuer (PPSI), mandates fully backed and bankruptcy remote reserves, sets enforceable redemption and liquidity expectations, introduces a rebuttable presumption against indirect yield-generating arrangements, and outlines a supervisory framework for foreign issuers. The OCC also finalized a related rule clarifying national trust bank chartering authority.[2]

The Federal Deposit Insurance Corporation (FDIC) has taken a narrower but strategically important path, issuing two complementary NPRs that together define how state-chartered institutions may enter the PPSI regime. The first issued December 19, 2025, establishes application and approval procedures for insured state nonmember banks and state savings associations, focusing on chartering mechanics, supervisory approvals, and operational readiness.[3] The comment period was set to close on February 17, 2026, but was extended to May 18, 2026.[4]

Editor's Note: In the May–June 2026 issue of ABA Risk and Compliance, the author examines the Act from a regulatory framework perspective. This second article shifts to what it means in practice — outlining the strategic decisions, operational demands, and competitive implications banks must address as the Act moves toward implementation.

The second, released on April 7, 2026, proposes prudential standards aligned with the Act's core requirements, including one-to-one reserve backing with eligible liquid assets, daily reserve monitoring, segregation of assets, two-business-day redemption timelines, and expectations for capital, liquidity, cybersecurity, and risk management.[5] The FDIC's framework is explicitly designed to dovetail with the OCC's rulemaking, signaling a consistent federal baseline for state-chartered institutions.

The National Credit Union Administration (NCUA) has likewise advanced its rulemaking, issuing a proposal focused on licensing and supervisory requirements for credit union affiliated entities seeking PPSI status.[6] The NPR outlines issuer eligibility standards tailored to credit union subsidiaries, governance and investment requirements aligned with the credit union regulatory framework, and integration with the Act's reserve, redemption, and operational expectations.

On April 8, 2026, the Financial Crimes Enforcement Network and the Office of Foreign Assets Control issued a joint proposed rule to implement provisions of the Act. As proposed, the rules will require PPSIs to meet full Bank Secrecy Act/Anti-money laundering (BSA/AML) and sanctions compliance obligations, treating them as financial institutions for purposes of AML controls, suspicious activity reporting, and sanctions enforcement. The proposal is framed as a balance between fostering innovation and protecting the U.S. financial system, ensuring that stablecoin issuers adopt programs capable of blocking, freezing, or rejecting illicit transactions while maintaining an sanctions compliance regime.[7]

The Department of the Treasury has taken a two-stage approach to implementing the Act's oversight framework. In September 2025, Treasury issued an NPR focusing, in part, on defining the Bank Secrecy Act and sanctions compliance obligations that will apply to payment stablecoin issuers, signaling early that BSA/AML expectations would be central to the new regime.[8] Treasury followed in April 2026, with another NPR outlining the criteria for determining whether state regulatory frameworks are "substantially similar" to federal standards, a foundational element of the Act's state certification model.[9] Together, these actions establish the federal baseline for both compliance obligations and state, federal supervisory alignment as the stablecoin ecosystem moves into the regulated perimeter.

"The Act is not merely a compliance mandate; it is the foundation of a new payments architecture in which digital dollars are expected to operate with the same safety, stability, and supervisory discipline as established financial instruments."

The Act is rapidly recasting the digital asset landscape into one defined by prudential standards, supervisory discipline, and operational transparency. As agencies race toward the July 18, 2026 rulemaking deadline, payment stablecoins are being formalized as a regulated payments instrument. That acceleration is forcing banks to confront strategic decisions that can no longer be deferred.

Strategic decisions facing banks

The Act is effectively compelling banks to declare their strategic posture in the emerging stablecoin ecosystem. The era of passive observation is over, and institutions must now determine how they intend to participate in a market that is rapidly becoming foundational to payments and liquidity. While a handful of banks may experiment across multiple fronts, most will ultimately concentrate their resources around one of five primary strategic pathways, each with distinct operational demands, regulatory implications, and competitive consequences.

Strategic option #1: Becoming a PPSI

Pursuing authorization as a PPSI is the most direct way for a bank to participate in the emerging stablecoin ecosystem, but it is also the path with the highest regulatory expectations and the greatest operational lift.[10] The Act treats stablecoin issuance as a core financial market infrastructure function, and regulators expect PPSIs to operate with the same rigor as systemically important payments providers. As a result, institutions considering this strategy must prepare to meet a set of demanding requirements across governance, risk management, technology, and compliance as discussed below.

Governance and organizational readiness

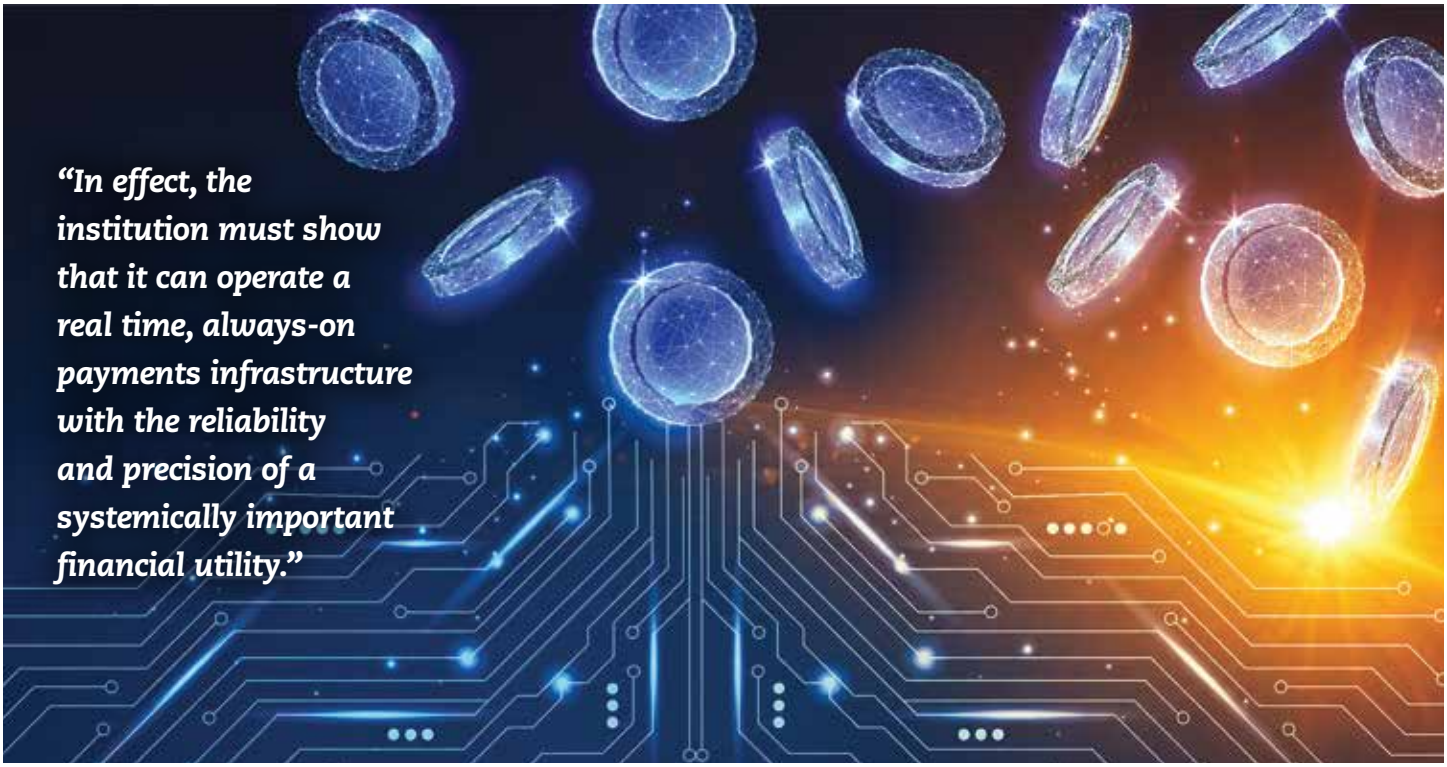
Becoming a PPSI demands a governance framework capable of withstanding sustained supervisory scrutiny and supporting continuous, high-velocity operations. Regulators expect banks to demonstrate mature, institution-wide oversight of stablecoin activities, beginning with a board that is explicitly accountable for issuance, reserve management, and redemption practices. That oversight must be reinforced by a senior management structure with clearly defined responsibility across technology, liquidity, risk, and compliance assuring that stablecoin operations are embedded within the bank's broader control environment rather than treated as an experimental or peripheral initiative.

To meet supervisory expectations, banks must also maintain robust internal controls, including segregation of duties, formal escalation protocols, and independent testing to validate the integrity of systems and processes.[11] Just as important, institutions must articulate a clear strategic rationale that shows how stablecoin issuance aligns with their business model, risk appetite, and long-term operational capabilities. In short, regulators will expect a bank to demonstrate not only that it can issue a stablecoin, but that it can do so safely, consistently, and at scale under conditions that mirror the demands of a critical payments infrastructure.

Reserve management and liquidity infrastructure

The Act imposes strict, nonnegotiable reserve requirements, obligating a PPSI to maintain high-quality and highly liquid assets backing every outstanding token on a one-to-one basis.[12] Meeting this standard requires ongoing liquidity monitoring, stress testing, and precise reconciliation processes, supported by independent

SHUTTERSTOCK / INACTIVE DESIGN



audits that validate the composition and valuation of the reserve portfolio. Institutions must also demonstrate operational readiness for real-time redemption, with the capacity to absorb large outflows without disrupting their balance sheet or broader financial stability.[13]

This is not a passive treasury function; it is an active liquidity-risk operation that mirrors the demands placed on money market funds and large scale payment processors. It requires continuous attention, disciplined controls, and resilient infrastructure.

Technology and operational infrastructure

Stablecoin issuance is, at its core, a technology-driven business operating within the framework of a regulated financial institution. To function as a credible issuer, a bank must build and maintain tokenization infrastructure capable of minting, burning, and tracking stablecoins across public or permissioned blockchains. That infrastructure must be tightly integrated with real-time ledgering and reconciliation systems so that on-chain activity aligns seamlessly with the bank's core systems of record. The technology stack must also meet high standards for cybersecurity and operational resilience, with redundancy, incident response capabilities, and continuous monitoring designed to support uninterrupted, high-volume activity. Equally important is the development of scalable APIs and settlement rails that enable merchant acceptance, wallet connectivity, and institutional transaction flows.

Regulators will expect a bank to demonstrate that this end-to-end technology environment can support continuous issuance and redemption without outages, data integrity failures, or operational bottlenecks.[14] In effect, the institution must show that it can operate a real-time, always-on payments infrastructure with the reliability and precision of a systemically important financial utility.

Compliance, risk, and supervisory expectations

The comprehensive compliance regime under which PPSIs will operate reflects the Act's expectation that stablecoin issuance function with the rigor of a critical payments utility. This includes full Bank Secrecy Act (BSA) and sanctions compliance, supported by blockchain analytics-enabled transaction monitoring capable of identifying illicit activity across on-chain and off-chain flows.[15] Consumer protection obligations must be met. These include the provision of clear redemption rights and transparent disclosures that ensure users understand how the stablecoin operates, and how reserves are managed.[16] The regulatory framework further imposes strict activity limitations, prohibiting lending, rehypothecation, or any speculative use of reserves to preserve the integrity and liquidity of the backing assets.[17] In addition, PPSIs are required to provide ongoing reporting such as reserve attestations, operational metrics, and incident notifications to give supervisors continuous visibility into the issuer's risk profile and operational performance.[18]

Taken together, these expectations create a materially higher compliance burden than traditional payments products. Regulators will expect any bank pursuing this model to demonstrate that it can manage the risks of a 24/7, globally accessible instrument with the same discipline, transparency, and operational maturity demanded of systemically important financial infrastructure.

Capital, risk appetite, and strategic commitment

Issuing a stablecoin is not a side project; it is a capital-intensive, multiyear strategic commitment. A PPSI must dedicate sufficient financial resources to absorb operational, legal, and reputational risks, supported by a clearly defined risk appetite that accounts for liquidity shocks, cyber events, and periods of market-wide stress.[19] The undertaking also requires a long investment horizon, as institutions must build and refine infrastructure, establish partnerships,

ISTOCK / INKOLY

and scale distribution channels before meaningful network effects emerge. Just as important is a coherent commercial strategy that articulates how the bank intends to monetize issuance, settlement, liquidity services, and broader participation in the stablecoin ecosystem.

Only institutions with strong operational capabilities, a durable balance sheet, and a compelling strategic rationale are likely to pursue this path, and regulators will expect banks to demonstrate that they can sustain the demands of a 24/7, high-velocity payments instrument over time.

Strategic option #2: Providing digital asset custody or operational services to issuers

Banks can indeed leverage their strengths in safekeeping, liquidity management, and disciplined risk controls to support stablecoin issuers without assuming the full obligations of a PPSI. But stepping into the role of a digital asset custodian introduces a different set of strategic challenges, most of them rooted in the information security demands of safeguarding cryptographic assets. Unlike traditional custody, where control is anchored in legal documentation and physical or electronic recordkeeping, digital asset custody hinges on the protection of private keys. This shifts the risk profile dramatically; a single compromise can result in irreversible loss, immediate customer harm, and significant reputational damage.

To operate credibly in this space, a bank must build an information security architecture that can withstand persistent, well-resourced cyber threats.[20] That includes hardened key management systems, secure enclave technologies, multiparty computation or hardware security module-based signing workflows, and strict segregation of operational environments. Continuous monitoring, anomaly detection, and blockchain analytics-enabled surveillance become essential, not optional. The bank must also be prepared for adversaries who target not just systems, but personnel — through social engineering, credential harvesting, and insider compromise. As a result, digital asset custody requires a level of operational discipline and cyber resilience that exceeds what most institutions deploy for traditional securities or cash management.

Strategically, this means banks must reconcile their appetite for participating in the digital asset ecosystem with the reality that custody is a 24/7, high-stakes security function. It demands sustained investment in talent, technology, and incident response capabilities, along with governance structures that can demonstrate to regulators that the bank maintains exclusive control over customer assets at all times. For institutions with established custody operations or strong treasury functions, the model is attractive — but only if they are prepared to elevate their information security posture to match the threat environment. In practice, the decision to custody digital assets is less about extending existing capabilities and more about committing to operate at the security standard of a critical financial market infrastructure.

Strategic option #3: Partnering with fintech or crypto-native issuers

Partnership models mirror the early years of open banking with banks providing regulated infrastructure, while fintechs provide distribution, user experience, and product innovation. This approach allows banks to participate in the stablecoin market without building end-to-end capabilities. It also positions banks as trusted intermediaries in a market where regulatory compliance and consumer protection are increasingly important.

The strategic advantages of the partnership approach start with an accelerated market without the burden of full build-out. Banks can participate in the stablecoin ecosystem immediately by leveraging fintech partners for token issuance, wallet UX, and distribution. This avoids multi-year investments in tokenization infrastructure, blockchain engineering, and specialized operational controls that Act-compliant issuers must maintain. Banks bring depth of experience in prudential oversight, consumer protection, and operational integrity as the regulated backbone overseeing Know Your Customer (KYC)/AML, reserve management, liquidity controls, and supervisory reporting, all indispensable to fintech partners and end-users.

Fintechs can iterate on user experience, programmability, and new use cases at a pace banks typically cannot match. The partnership model allows banks to benefit from this innovation while maintaining a controlled risk perimeter aligned with their supervisory expectations.

Banks can view these partnerships as proving ground. If stablecoin volumes scale or regulatory clarity increases, banks can selectively insource capabilities in reserve management, token issuance, or on-chain settlement without having overcommitted capital prematurely. Moreover, banks can generate fee-based revenue from custody, settlement, compliance services, and API-based infrastructure without taking on the full operational burden of becoming an Act-registered issuer.

In terms of strategic drawbacks, by placing dependence on fintech partners for executing on customer experience and growth, banks risk ceding to fintech partners the most valuable aspect of the value chain — distribution of products, services and customer engagement. Over time, this may limit brand visibility, customer ownership, and the ability to shape emerging stablecoin use cases. Even when fintechs handle front-end functions, regulators will expect banks to maintain oversight, vendor-risk governance, and compliance assurance.[21] This creates asymmetric responsibility where banks bear supervisory risk for activities they do not fully control.

If many banks adopt the same model, the regulated-infrastructure layer could become

ISTOCK / RAWPIXEL

commoditized. This may limit influence over product design and banks may be constrained in shaping token features, interoperability standards, or programmability attributes, all areas that will define competitive differentiation as the market matures.

There also is the potential for misalignment of risk appetite and pace of innovation. Fintechs may push aggressively into new use cases such as cross-border settlement, embedded finance, and corporate treasury automation, exceeding a bank's risk tolerance or supervisory comfort and straining partnerships.

The partnership route offers banks a sensible, low-commitment way to establish a foothold in the Act era. The partnership model is a pragmatic, low-friction entry point for banks navigating the Act's early regulatory landscape. It allows institutions to participate in stablecoin markets quickly, credibly, and with manageable investment. But it may not be a long-term strategy by default. Banks might view this as a transitional posture, one that preserves options while allowing time to evaluate whether to evolve into full issuers, specialized settlement providers, or orchestrators of the broader tokenized economy.

Strategic option #4: Focusing on tokenized deposits

Some institutions may decide that tokenized bank liabilities, rather than stablecoins, better align with their risk appetite and supervisory expectations. Tokenized deposits offer many of the same benefits as stablecoins (speed, programmability, interoperability) while remaining fully within the traditional banking framework. For banks that want to modernize payments without entering the stablecoin market directly, tokenized deposits may be the preferred path.

There are plenty of arguments favoring industry investment in supporting tokenized deposits versus direct involvement in stablecoins. The main argument most often waged is that tokenized deposits preserve deposit base and that stablecoins risk disintermediation. Stablecoins can reduce, restructure, or displace bank deposits depending on adoption patterns, reserve allocation, and whether issuers gain master account access. If stablecoins substitute for bank deposits, banks lose funding. Deposit outflows to stablecoins reduce credit supply through balance sheet contraction, higher funding costs, liquidity buffer requirements, and maturity transformation constraints. It is estimated that for every $100 billion net deposit drain, this reduces lending by $60 billion to $126 billion, with additional reductions from composition effects. Tokenized deposits preserve the deposit-to-loan multiplier, while PPSI adoption erodes banks' ability to extend credit.[22]

Arguments aside, a balanced path is emerging in which tokenized deposits and payment stablecoins evolve as complementary, not competing, instruments. In this middle-ground model, tokenized deposits remain the primary on-chain expression of commercial bank money, supporting insured retail and commercial payments, prudentially supervised balance sheet activity, and on-chain settlement for customers who want blockchain functionality without exiting the banking system. Stablecoins, by contrast, occupy the open-loop, platform-native domain, powering global marketplaces, cross-border flows, and decentralized finance. Rather than forcing a binary choice, each instrument can meet specific market needs when optimized for its respective environment. In this model, tokenized deposits anchor the regulated financial system, while PPSIs extend programmability and reach into broader digital ecosystems.

Strategic option #5: Monitoring from the sidelines

Observing from the sidelines as a strategy may be viable in the short term, particularly for institutions assessing demand, regulatory clarity, or competitive fit. But it carries significant risks. Financial institutions that move early will shape customer expectations, build partnerships, and establish market share. Those that wait may find themselves competing on someone else's terms.

Strategic implications by bank segment

Community banks: Niche opportunities, real constraints

Community banks face both opportunity and risk. On one hand, they can carve out roles in local market use cases, such as supporting small business payments, community-based fintech partnerships, or regional economic development initiatives. On the other hand, scale, technology investment, and supervisory expectations may limit the ability of smaller financial institutions to issue stablecoins directly.

True to the times, a realistic, viable path for community banks is often collaboration. This approach leverages third-party infrastructure while maintaining customer relationships. By partnering with fintechs, core providers, or consortiums, community banks can offer stablecoin-enabled services without building the underlying technology themselves.

Regional banks: Modernization under pressure

Regional banks sit in the most competitively pressurized position. Banks in this size category must modernize infrastructure to remain relevant in treasury services, payments, and commercial banking. They face pressure from money-center banks with scale and from fintechs with speed. Stablecoin-enabled services could become a differentiator if they move decisively.

For regional banks, the Act is less about issuing stablecoins and more about upgrading capabilities related to blockchain connectivity, real-time settlement, digital asset custody, and enhanced compliance. Institutions that invest early will be better positioned to compete for corporate clients seeking faster, programmable, and globally interoperable payment solutions.

Money-center banks: Scale and execution

Large banks have balance sheets, global networks, and operational sophistication to issue stablecoins at scale. They are also best positioned to integrate stablecoins into wholesale settlement, cross-border payments, and liquidity management. But they face the highest expectations from regulators and the market.

For money-center banks the challenge is not a question of capability; it is about speed and time to market. Delay in adopting risks allowing fintechs and crypto firms to define the market before banks fully engage. Money-center banks that move quickly can shape industry standards, influence regulatory expectations, and capture early mover advantages.

Preparing for the Act: Bank priorities for 2026

Regardless of strategic posture, banks must prepare for a new supervisory environment. Key priorities include:

Internal literacy and governance

Boards and executive managers must understand stablecoin mechanics, risks, and regulatory obligations. This understanding must translate to governance

structures updated to reflect new operational and compliance responsibilities. Banks that treat digital asset literacy as a strategic competency rather than a technical niche will be better positioned to make informed decisions.

Strategic fit assessments

Banks face a determination as to whether issuance, custody, partnership, tokenized deposits, or some combination of digital products and services align with their business model, customer base, and risk appetite. Cross-functional input will be essential to assessing these business models. Making a business decision of this magnitude and complexity cannot be treated as a siloed strategic exercise. Each pathway touches multiple risk domains, operational dependencies, and regulatory expectations. To effectively navigate this decision, the process must engage:

- Strategy to evaluate market opportunity, competitive positioning, and whether stablecoin participation advances the bank down a broader digital asset roadmap.
- Risk management to assess operational, liquidity, credit, third-party, model, and reputational risks, each of which manifests differently across issuance, partnership, and tokenized deposit models.
- Compliance to interpret the Act and the implementing regulations, supervisory expectations, BSA/AML and sanctions obligations, and the heightened scrutiny applied to bank-fintech business model arrangements supporting on-chain activities.
- Technology to determine whether existing infrastructure can support on-chain settlement, wallet integrations, reserve reporting, and real-time monitoring or whether system upgrade and modernization is required.
- Treasury to evaluate reserve composition, liquidity implications, intraday settlement flows, and how stablecoin liabilities interact with the bank's balance sheet strategy.

No single functional area has a full picture. Only a coordinated assessment can determine whether the bank's capabilities, economics, and risk posture align with the demands of stablecoin issuance, the constraints of partnership, or the operational logic of tokenized deposits.

Technical readiness

Stablecoin-enabled services introduce a set of capabilities that extend well beyond traditional banking infrastructure. Banks must be prepared to support wallet functionality for customers and counterparties, including key management, address whitelisting, and transaction-level controls.[23] Additionally, robust blockchain connectivity, with nodes, monitoring tools, and analytics that allow real time visibility into on-chain activity will factor into overall readiness. Effective reserve management systems are essential to track assets, reconcile flows, and meet the Act's reporting requirements. In parallel, banks must implement smart contract governance frameworks to oversee contract deployment, versioning, permissions, and auditability. All of this must coexist within cybersecurity controls tailored to digital asset risks, including private key protection, multiparty computation, and enhanced monitoring for on-chain threats.

Given the breadth and specialization of these requirements, banks must make deliberate decisions about whether to build, buy, or partner for each capability, while balancing speed, control, cost, and regulatory expectations as they shape their long-term digital asset strategy.

Vendor due diligence

Banks evaluating whether to become a PPSI must treat vendor due diligence as a strategic capability, not a compliance formality. The PPSI model depends on a tightly integrated ecosystem of blockchain analytics firms, custody providers, wallet vendors, and smart contract auditors, each introducing operational dependencies that regulators will scrutinize. The strategic question is not simply whether a vendor is "adequate" but whether the bank can demonstrate credible, end-to-end control over a technology stack that operates continuously, globally, and with little tolerance for error.

Blockchain analytics partners, for example, become extensions of the bank's financial crime program. Their methodologies, data sources, and false positive rates directly influence the bank's ability to detect illicit activity on-chain. Custody providers raise questions about key management models, segregation of duties, and the bank's ability to evidence exclusive control over customer assets. Wallet vendors shape the customer experience and the bank's exposure to device-level vulnerabilities, while smart contract auditors determine whether the bank can defend the integrity of the token itself. Each relationship therefore affects not only risk but also the bank's credibility with supervisors, counterparties, and the market.[24]

Strategically, banks must decide whether to build, buy, or partner for these capabilities — and how those decisions align with long-term ambitions in digital assets. Overreliance on a single vendor may accelerate time-to-market but creates concentration risk and weakens negotiating leverage. A multivendor model improves resilience but increases integration complexity and oversight demands. Banks must also consider how vendor choices signal maturity, as regulators will expect evidence that the bank selected providers based on rigorous criteria, validated controls, and established monitoring mechanisms capable of supporting a 24/7 issuance and redemption environment.

In short, vendor due diligence for PPSI candidates is not a back-office exercise. It is a strategic design decision that shapes the bank's risk posture, regulatory defensibility, and long-term ability to operate a stablecoin program safely and at scale.

Wallet and custody capabilities

Whether built or outsourced, digital asset safekeeping becomes a core competency. Banks must evaluate custody models, insurance coverage, segregation of assets, and operational controls.

Whether developed internally or sourced through a third-party provider, digital asset safekeeping becomes a foundational competency for any bank operating as a PPSI. The bank must evaluate not only the technical custody model, but also how that model supports continuous issuance, redemption, and settlement obligations. Insurance coverage, asset segregation, and operational controls take on heightened importance because the bank must be able to demonstrate exclusive control over private keys and uninterrupted access to customer assets.[25]

Strategically, custody design choices shape the bank's entire risk posture. Decisions about wallet architecture influence customer experience, fraud exposure, and the bank's ability to enforce address-level controls. Key management workflows determine resilience against insider threats and external compromise. The bank must also assess how custody and wallet infrastructure integrate with broader governance requirements such as smart contract permissions, reserve management systems, and blockchain monitoring tools, so that the stablecoin program operates as a coherent, defensible whole.

In effect, custody is no longer a supporting function; it becomes the operational core of the PPSI model. Banks must therefore treat wallet and safekeeping capabilities as strategic infrastructure that must withstand supervisory scrutiny, adversarial threat environments, and the demands of a 24/7 digital asset ecosystem.

Compliance and risk priorities under the Act

The Act establishes a distinctly new compliance perimeter for banks, requiring traditional control frameworks to evolve in ways that reflect the realities of blockchain-based financial activity. Core compliance management systems must be expanded to incorporate blockchain data, smart contract risks, and digital asset transaction monitoring, transforming crypto oversight from an add-on into an integrated component of the bank's Compliance Management System (CMS). Moreover, transaction monitoring must also be strengthened, as blockchain transactions introduce novel typologies such as cross-chain transfers, decentralized exchange activity, and deliberate obfuscation techniques that demand enhanced monitoring, analytics, and escalation protocols.

At the same time, banks must conduct stablecoin-specific risk assessments covering liquidity, operational, cybersecurity, and consumer protection risks unique to tokenized liabilities. These assessments will anchor dialogue with regulators and shape the bank's risk management posture. Banks will be expected to deploy blockchain analytics capable of tracing activity across chains and through obfuscation layers, implement high risk transaction detection models tuned to digital asset typologies, and build investigative processes that integrate on-chain and off-chain data.[26] Regulators will expect nothing less.

The road ahead: A strategic inflection point

Stablecoins are rapidly maturing into both a next generation payments rail and a programmable liquidity layer, and the Act is accelerating their movement into the regulated core of U.S. finance. The competitive landscape is already reshaping itself as banks, fintechs, and crypto-native issuers position for scale, market share, and institutional trust.

"For banks, 2026 is not simply another planning cycle — it is a strategic breakpoint and a genuine sea change in how value will move through the financial system."

For banks, 2026 is not simply another planning cycle — it is a strategic breakpoint and a genuine sea change in how value will move through the financial system. Institutions that choose to lead will shape the architecture of the next payments era. Institutions that choose to lead will shape the architecture of the next payments era. Those that partner will need to move with precision and speed. Those that wait risk watching the center of gravity shift without them. The Act is far more than a compliance mandate. It is a catalyst to modernize infrastructure, assert competitive differentiation, and reclaim the role of banking at the center of a financial system that is rapidly becoming digital. ■

ABOUT THE AUTHOR

THOMAS GRUNDY, CRCM is the Director, US Regulatory Consulting at Wolters Kluwer. Tom joined Wolters Kluwer in 2013 and has over forty years' experience spanning federal regulation, financial industry compliance, and advisory consulting. His career includes service as a federal regulator with both the Office of the Comptroller of the Currency and the Federal Reserve Board, as well as senior compliance roles within banking, mortgage, and fintech organizations. Tom draws on this diverse background to advise financial institutions on strategies and solutions that strengthen risk management and support sound, sustainable compliance in a dynamic regulatory landscape.

Tom is a graduate of the University of Kentucky, the Graduate School of Banking at the University of Wisconsin, and the American Bankers Association National Graduate Compliance School and is a Certified Regulatory Compliance Manager. Reach him at thomas.grundy@wolterskluwer.com and (270)402-9069.

Endnotes

1. https://www.occ.treas.gov/news-issuances/bulletins/2026/bulletin-2026-3.html
2. https://www.occ.treas.gov/news-issuances/bulletins/2026/bulletin-2026-4.html
3. https://www.fdic.gov/news/financial-institution-letters/2025/notice-proposed-rulemaking-establish-genius-act-application
4. https://www.fdic.gov/news/press-releases/2026/fdic-extends-comment-period-proposal-establish-GENIUS-act-application
5. https://www.fdic.gov/news/financial-institution-letters/2026/notice-proposed-rulemaking-establish-genius-act
6. https://ncua.gov/newsroom/press-release/2026/ncua-proposes-rule-permitted-payment-stablecoin-issuer-applications
7. https://home.treasury.gov/news/press-releases/sb0435
8. https://www.federalregister.gov/documents/2025/09/19/2025-18226/genius-act-implementation
9. GENIUS Act §§3—5; see also U.S. Department of the Treasury, Permitted Payment Stablecoins: Supervisory and Prudential Standards, Notice of Proposed Rulemaking, 91 Fed. Reg. 16844, 16847—48 (Apr. 3, 2026)
10. GENIUS Act §4
11. 12 USC §5903(a)
12. 12 USC §5903(a)(1)(A)
13. 12 USC §5903(a)(1)(C); 12 USC §5903(a)(3)
14. 12 USC §5903(a)(4)(A)(iv)
15. ibid.
16. 12 USC §5903(a)(1)(B)(i) -(ii)
17. 12 USC §5903(a)(2)
18. 12 USC §5903(a)(1)(C); 12 USC §5903(a)(3)(B)
19. 12 USC §5903(a)(4)
20. https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic19-encryption/
21. https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf
22. https://www.federalreserve.gov/econres/notes/feds-notes/banks-in-the-age-of-stablecoins-implications-for-deposits-credit-and-financial-intermediation-20251217.html
23. https://occ.gov/topics/charters-and-licensing/interpretations-and-decisions/2020/int1170.pdf; https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic19-encryption/; https://www.fdic.gov/interagency-statement-crypto-asset-safekeeping.pdf
24. https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management
25. https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20250714a1.pdf
26. Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets, March 2026, United States Department of the Treasury