GEORGETOWN UNIVERSITY
Psaros Center for Financial Markets and Policy
McDONOUGH SCHOOL of BUSINESS

Stablecoins and the Rising Need for Confidential Blockchain Transactions

Yaya J. Fanusie
Visiting Fellow

Julen Payne
Research Assistant

Georgetown University's Psaros Center for Financial Markets and Policy

McDonough School of Business
July 2026

Executive Summary

The Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), signed into law in July 2025, represents Congress's first comprehensive effort to regulate payment stablecoins. By establishing reserve requirements, consumer protections, and a dual-track federal-state supervisory structure, the Act creates a credible path for institutional adoption of stablecoins in payments, settlement, and treasury operations. Yet the Act leaves a critical gap unaddressed: it says nothing about how stablecoin issuers should protect customer transaction privacy on public blockchains.

This silence creates a structural problem. Public blockchains—the infrastructure on which most stablecoins operate—make every transaction permanently and publicly visible. The GENIUS Act subjects stablecoin issuers to Bank Secrecy Act (BSA) obligations and, for those supervised by the Office of the Comptroller of the Currency (OCC), to Gramm-Leach-Bliley Act (GLBA) requirements to protect nonpublic personal information. On a transparent blockchain, GLBA obligations present a structural challenge: every transaction is publicly visible, making it difficult for issuers to protect customer financial information required by law. Importantly, privacy-preserving technology does not undermine BSA compliance—it can enhance it, by enabling targeted, cryptographically verifiable disclosure to regulators rather than relying on raw public ledger data. The OCC's proposed rule implementing the Act compounds this problem by defining distributed ledger data as "publicly available information," effectively excluding on-chain transaction records from the privacy protections that would otherwise apply to the same customer financial data held by any other OCC-supervised institution.

This paper argues that privacy-preserving technology is not merely a market preference for the stablecoin industry—it is a regulatory necessity. It examines the GENIUS Act's privacy gap, the growing attention from federal regulators, the legal obligations that already require transaction confidentiality, and the emerging technological approaches that can close this gap while maintaining compliance with anti-money laundering and sanctions requirements.

I. The GENIUS Act and the Privacy Gap It Creates

A. What the GENIUS Act Does

The GENIUS Act became law on July 18, 2025, following bipartisan votes in both chambers of Congress.[1] It establishes the first comprehensive federal regulatory framework for payment stablecoins—digital assets designed to maintain a stable value relative to a fixed amount of monetary value, redeemable on demand at par. The Act requires issuers to maintain 100% reserve backing in cash, Treasury securities, or central bank deposits. It creates a dual-track regulatory structure: the OCC oversees federally chartered nonbank

[1]Guiding and Establishing National Innovation for U.S. Stablecoins Act, S. 1582, 119th Cong. (2025) (signed into law July 18, 2025); Congressional Research Service, "The GENIUS Act: Stablecoin Legislation," IN12553, July 18, 2025, https://www.congress.gov/bill/119th-congress/senate-bill/1582/text.

issuers, while state regulators may supervise issuers with less than $10 billion in outstanding stablecoins, provided the state regime is certified as "substantially similar" to the federal framework. The Act will take effect no later than January 18, 2027, or sooner if final implementing regulations are issued and 120 days elapse. It explicitly excludes compliant payment stablecoins from the definitions of "security" and "commodity" to remove them from the jurisdiction of the Securities and Exchange Commission and the Commodity Futures Trading Commission, respectively.[2]

The regulatory clarity the GENIUS Act provides is expected to accelerate institutional adoption of stablecoins across a range of financial applications. Cross-border settlement, interbank payments, treasury operations, payroll, and business-to-business supply chain payments all stand to benefit from the Act's supervisory framework and consumer protections. Major banks have signaled intent to issue stablecoins through subsidiaries, and payment infrastructure companies are already integrating stablecoin capabilities into their networks.[3]

B. The Privacy Gap

The GENIUS Act subjects all permitted stablecoin issuers to Bank Secrecy Act (BSA) obligations.[4] It requires the Financial Crimes Enforcement Network (FinCEN) to develop tailored anti-money laundering rules for the stablecoin sector. Notably, the Act also directs FinCEN to facilitate "novel methods … to detect illicit activity involving digital assets"—an implicit acknowledgment that existing surveillance tools may be insufficient for digital asset infrastructure.[5] Following a public comment process that drew more than 220 responses from industry, Treasury delivered its findings in a March 2026 report to Congress on innovative technologies to counter illicit finance, which endorsed the development of novel detection tools, including privacy-preserving approaches.[6]

What the GENIUS Act does not address is how stablecoin issuers should handle the privacy of customer transaction data on public blockchains. The Act creates financial institution obligations—under the BSA and, for OCC-supervised entities, under the

[2]GENIUS Act § 4(a)(1)–(3) (defining "payment stablecoin" as a digital asset designed to be used as a means of payment or settlement, denominated in a national currency, and redeemable at a fixed amount of monetary value); § 4(b) (reserve requirements); § 3 (dual-track regulatory structure); § 12 (effective date: no later than January 18, 2027, or 120 days after final implementing regulations); § 8 (exclusion from the definitions of "security" under the Securities Act of 1933 and "commodity" under the Commodity Exchange Act).

[3]See, e.g., Yaya J. Fanusie & Saskia Seidel, "Considering Institutional DeFi Integration: How To Manage Illicit Finance Risk," Georgetown Psaros Center for Financial Markets and Policy, October 2025.

[4]GENIUS Act § 6 (requiring permitted payment stablecoin issuers to comply with the Bank Secrecy Act, 31 U.S.C. § 5311 et seq.).https://finpolicy.georgetown.edu/wp-content/uploads/2025/10/Considering-Institutional-DeFi-Integration_-How-To-Manage-Illicit-Finance-Risk_FINAL.docx.pdf

[5]GENIUS Act § 6(b)(2) (directing the Financial Crimes Enforcement Network to facilitate "novel methods … to detect illicit activity involving digital assets").

[6]U.S. Department of the Treasury, Report to Congress on Innovative Technologies to Counter Illicit Finance Involving Digital Assets, March 2026, https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf. The report was preceded by a public Request for Comment issued in August 2025, which drew more than 220 responses from industry.

Gramm-Leach-Bliley Act (GLBA)—without accounting for the fact that the underlying infrastructure makes all transactions visible to anyone with internet access.

The vast majority of stablecoins today operate on public blockchains such as Ethereum, Solana, and Tron, where every transaction is permanently and publicly recorded. This transparency is fundamentally incompatible with the privacy expectations embedded in existing financial regulation and with the practical requirements of institutional adoption. Consider a straightforward scenario: a company paying contractors in stablecoins on a public blockchain would expose every payment amount, every counterparty, and every balance to competitors, employees, and the general public. No chief financial officer would accept that arrangement. Yet this is the default condition of stablecoin payments today.

II. Regulators Are Taking Notice

A. The SEC Roundtable on Financial Surveillance and Privacy

The tension between blockchain transparency and financial privacy is not merely an industry concern. Federal regulators are now actively engaging with it. On December 15, 2025, the Securities and Exchange Commission's (SEC's) Crypto Task Force convened a roundtable on "Financial Surveillance and Privacy," with both SEC Chairman Paul Atkins and Commissioner Hester Peirce delivering remarks that framed the issue as a first-order policy question.

Chairman Atkins opened the roundtable by framing the discussion around what he called a "profoundly American" question: "whether people can participate in modern finance without surrendering their privacy."[7] He warned that if the instinct of government is to treat every wallet like a broker, every protocol as a surveillance node, and every transaction as a reportable event, public blockchains could become "the most powerful financial surveillance architecture ever invented." Atkins critiqued the SEC's own data collection tools—including the Consolidated Audit Trail, Form PF, and swap data repositories—as having expanded beyond their original purposes in ways that put investor privacy at risk.[8] He also made a market structure argument that is directly relevant to stablecoin adoption: complete financial transparency disincentivizes institutional activity, because market participants cannot build positions, execute hedging strategies, or conduct underwriting if every flow is visible in real time to competitors.[9] Atkins affirmatively endorsed cryptographic tools like

[7]SEC Chairman Paul S. Atkins, Remarks at the Crypto Task Force Roundtable on Financial Surveillance and Privacy, December 15, 2025.https://www.sec.gov/newsroom/speeches-statements/atkins-121525-remarks-crypto-task-force-roundtable-financial-surveillance-privacy

[8]Id.

[9]Id. ("[M]any institutions depend on the ability to build positions discreetly before disclosing them. If a large asset manager's strategy is visible in real time on a public ledger, competitors can front-run those trades, driving up prices before the manager can execute.").

zero-knowledge proofs,[10] which enable users to demonstrate compliance with a specific data requirement without surrendering their entire transaction history or identity information.

Commissioner Peirce reinforced these themes and connected them directly to the GENIUS Act. She noted that Congress, through the Act's FinCEN directive, has already signaled that novel detection methods are needed—and that privacy-preserving tools such as zero-knowledge proofs merit serious regulatory engagement rather than reflexive suspicion.[11] Peirce articulated a set of normative principles: government should not assume illicit intent when people guard their financial privacy; it should not force the creation of intermediaries solely for surveillance purposes; and BSA obligations should not attach to software developers who do not custody user assets.[12]

In an earlier speech at the Berkeley Center for Law, Business, and the Economy in August 2025,[13] Peirce provided deeper legal grounding for this position, tracing the erosion of financial privacy from the third-party doctrine in *Smith v. Maryland* through the Supreme Court's reassessment in *Carpenter v. United States*.[14] She connected the BSA's fifty-five-year expansion to what she described as a "national degradation of financial privacy" that is "overdue for a change," and argued that the advent of digital assets is helping to catalyze that reassessment.

B. A Window for Reassessment

The convergence of stablecoin legislation, SEC engagement, and the Department of Treasury's focus on compliance innovation creates a rare window to rethink how financial surveillance is conducted. Digital assets enable a fundamentally different approach: compliance can be embedded in infrastructure—through cryptographic proofs and programmable disclosure—rather than layered on top through intermediary reporting obligations that were designed for the analog era.

The breadth of engagement with Treasury's public comment process reflects how widely this concern is shared. Responses came from venture capital firms, industry associations, stablecoin issuers, and identity infrastructure providers—a cross-section of the digital asset ecosystem that includes both the builders of privacy-preserving technology and the regulated institutions that will need to deploy it. Treasury's March 2026 report to Congress synthesized those views and signaled affirmative support for innovative detection methods,

---

[10] A zero-knowledge proof is a cryptographic method that allows one party to prove to another that a statement is true — for example, that a transaction is valid or that a user meets a compliance threshold — without revealing any of the underlying information.

[11] SEC Commissioner Hester M. Peirce, Remarks at the Crypto Task Force Roundtable ("Privacy in the House"), December 15, 2025. https://www.sec.gov/newsroom/speeches-statements/peirce-remarks-crypto-task-force-roundtable-121525

[12] Id.

[13] SEC Commissioner Hester M. Peirce, "Peanut Butter & Watermelon: Financial Privacy in the Digital Age," Remarks at the Berkeley Center for Law, Business, and the Economy Annual Conference, August 4, 2025. https://www.sec.gov/newsroom/speeches-statements/peirce-remarks-blockchain-conference-080425

[14] Id. (discussing Carpenter v. United States, 585 U.S. 296 (2018), and the evolution of the third-party doctrine).

including privacy-preserving approaches. The question is no longer whether financial privacy matters in a stablecoin regime. It is how to achieve it.[15]

III. Why Stablecoin Issuers Must Develop Privacy-Preserving Measures

A. Use Cases That Require Confidentiality

The practical case for transaction privacy is straightforward. No employer paying workers in stablecoins can allow salary information to be publicly visible on a blockchain. No business conducting supply chain payments can expose vendor pricing, contract terms, and payment timing to competitors. No financial institution will move treasury operations, trading, or settlement on-chain if counterparties can observe every position, every hedge, and every flow in real time—a concern that Chairman Atkins highlighted as a structural market risk. Lending and credit markets require borrower confidentiality. Even basic consumer payments require that purchase history, account balances, and counterparties remain private. In short, no category of serious financial activity can function on a fully transparent ledger. The privacy problem is not a niche concern—it is a prerequisite for the institutional adoption that the GENIUS Act is designed to enable.

B. Existing Regulatory Obligations Already Require Privacy Protection

The case for privacy-preserving stablecoins does not rest solely on market demand. Existing law already requires it. Stablecoin issuers supervised by the OCC are subject to the GLBA,[16] which prohibits financial institutions from disclosing nonpublic personal information (NPI) to nonaffiliated third parties unless the institution provides notice and the consumer is given a reasonable opportunity and reasonable means to opt out of such disclosures. The OCC's Comptroller's Handbook[17] specifies examination procedures to ensure that supervised institutions comply with these requirements. NPI, as defined under GLBA, includes transaction data, account numbers, and balances—precisely the categories of information that are permanently and publicly visible on a transparent blockchain.[18]

On a public blockchain, every transaction is effectively a disclosure to the entire world. There is no opt-out mechanism. A consumer cannot direct her stablecoin issuer to withhold transaction data from nonaffiliated third parties because the ledger itself makes that data

[15]See Treasury RFC responses from Andreessen Horowitz (a16z), Ribbit Capital, Crypto Council for Innovation (CCI), Circle Internet Group, and Persona, Inc. (2025). See https://www.regulations.gov/docket/TREAS-DO-2025-0070/comments; see also Treasury, March 2026 Report to Congress, supra note 6.
[16]Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 502, 113 Stat. 1338 (1999) (codified at 15 U.S.C. § 6802). https://www.govinfo.gov/app/details/PLAW-106publ102
[17]Office of the Comptroller of the Currency, Comptroller's Handbook: Privacy of Consumer Financial Information, October 2011. https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/privacy-consumer-financial-info/pub-ch-privacy.pdf
[18]Id. ("nonpublic personal information" includes financial information provided by a consumer, resulting from a transaction with the consumer, or otherwise obtained in connection with providing a financial product or service).

available to everyone. This is the compliance gap: the GENIUS Act subjects stablecoin issuers to financial institution obligations that presuppose the ability to control the flow of customer information, while the infrastructure on which most stablecoins operate provides no such control.

The OCC's proposed rule implementing the GENIUS Act confirms this gap.[19] The proposed rule defines "publicly available information" to explicitly include data from distributed ledgers.[20] Because the rule's NPI protections exclude publicly available information, on-chain transaction data falls outside those protections by design—regardless of whether the issuer had the technical means to prevent that data from becoming public in the first place. The result is anomalous and unprecedented in traditional banking: a customer's complete payment history becomes permanently and publicly searchable, yet is excluded from the privacy framework that was designed to protect exactly that kind of information. In its comment letter on the proposed rule, the Aleo Network Foundation[21] argued that issuers who have the technical capability to shield customer transaction data should bear an affirmative obligation to do so, and that the OCC should establish transaction confidentiality as a data privacy standard for permitted stablecoin issuers—not merely a best practice.[22]

Private stablecoins are not merely a market preference. They are a regulatory necessity. Without privacy-preserving technology, OCC-supervised stablecoin issuers will face a structural inability to comply with the consumer financial privacy obligations that have governed American banking for over two decades.

C. From Mixers to Compliant Privacy

The blockchain ecosystem's first attempts at transaction privacy were not designed for the regulated financial system. Mixers and tumblers arose in the Bitcoin ecosystem to obscure the origins of cryptocurrency transactions, initially motivated by the legitimate concern that large holders' wealth was visible on-chain to anyone. But these tools were quickly exploited for money laundering, as they could wash stolen or illicitly obtained cryptocurrency into new, untraceable addresses. The regulatory and enforcement response was severe: the Treasury Department sanctioned Tornado Cash in 2022, and the Department of Justice pursued criminal prosecutions against mixer operators. The lesson is clear: privacy tools that cannot distinguish between licit and illicit activity are inappropriate for the regulated financial system.[23]

A new generation of privacy-preserving technologies takes a fundamentally different approach. Rather than obscuring transactions after the fact, these systems build

[19]OCC, Notice of Proposed Rulemaking, Implementing the GENIUS Act for the Issuance of Stablecoins, Docket ID OCC-2025-0372. https://www.regulations.gov/docket/OCC-2025-0372
[20]Id. Proposed § 15.2 (defining "publicly available information" to include data from a distributed ledger).
[21] Disclosure: This paper's co-author Yaya J. Fanusie is Global Head of Policy at the Aleo Network Foundation.
[22]See Aleo Network Foundation, Comment Letter on OCC NPRM Docket ID OCC-2025-0372 (2026). https://aleo.org/post/occ-genius-letter/
[23]See U.S. Department of the Treasury, Office of Foreign Assets Control, Designation of Tornado Cash, August 8, 2022. https://home.treasury.gov/news/press-releases/jy0916

confidentiality into the infrastructure itself—at the protocol or chain level—while maintaining the ability to provide verifiable transaction records to regulators and auditors through cryptographic mechanisms such as selective disclosure.

Several operational examples illustrate the range of approaches. The Aleo Network is a Layer-1 blockchain with built-in programmable privacy, using zero-knowledge proofs to enable private transactions by default while supporting selective disclosure for compliance purposes through cryptographic view keys. Aleo has established formal integrations with Circle and Paxos Labs for stablecoin privacy solutions.[24] The Canton Network, developed by Digital Asset, is an enterprise-focused blockchain designed for institutional use, with privacy by design and granular data-sharing controls; major financial institutions have adopted it for settlement and synchronization of financial transactions.[25] Polygon Miden is a zero-knowledge rollup architecture that enables private transactions on Ethereum through client-side proving, allowing users to execute transactions privately while the network verifies their validity.[26]

The common thread across these approaches is that they allow users or institutions to prove regulatory compliance—including sanctions screening, identity verification, and transaction limits—without exposing the underlying transaction data to the public. This is the critical distinction from earlier privacy tools: compliance is not sacrificed for privacy, nor is privacy sacrificed for compliance. Both objectives can be achieved simultaneously through a well-designed cryptographic infrastructure.[27]

IV. Recommendations and Outlook

A. What Industry Must Do

The digital asset industry must build privacy-preserving solutions that are designed for regulatory compliance from the ground up. The lesson of mixers and tumblers is that privacy tools built without regard for anti-money laundering and sanctions requirements will not survive regulatory scrutiny and will ultimately harm the broader ecosystem's credibility. The standard must be privacy with compliance, not privacy despite compliance.

---

[24] See Aleo Network, https://aleo.org; see also Circle and Aleo partnership announcement (2025); Paxos Labs and Aleo integration (2025); Yaya J. Fanusie, Valerie-Leila Jaber, and Matthew Green, "Stablecoin Privacy: Balancing Privacy and Risk Through Permissionless Private Stablecoin Infrastructure," Aleo Network Foundation, June 2026, https://aleo.org/doc/aleo-stablecoin-whitepaper.pdf.

[25] See Canton Network, https://www.canton.network.

[26] See Polygon Miden, https://polygon.technology/polygon-miden.

[27] Like all modern cryptographic systems, zero-knowledge proofs rely on mathematical code that is almost impossible for today's computers to break—but could, in theory, become breakable by future quantum computers. This is a long-term consideration for all digital infrastructure, not unique to privacy-preserving technology, and cryptographers are already developing 'quantum-resistant' versions of these tools. The U.S. National Institute of Standards and Technology has been finalizing quantum-resistant cryptographic standards since 2024. Whether and how quickly privacy-preserving stablecoin infrastructure adopts these standards will be an important consideration as the technology matures. See National Institute of Standards and Technology, "Post-Quantum Cryptography FIPS Approved," August 13, 2024, https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved.

Industry participants should also prioritize partnerships between traditional financial institutions and privacy-focused blockchain developers. Banks and payment companies bring regulatory expertise, compliance infrastructure, and market access; blockchain developers bring cryptographic innovation and protocol design capabilities. These partnerships will be essential for developing solutions that work within the GENIUS Act's dual-track regulatory structure and across multiple blockchain ecosystems. Interoperability standards should be developed early, before fragmentation makes integration more difficult and costly.[28]

Finally, industry must engage actively with the regulatory process. Regulators are seeking input from the public on how to implement thethe GENIUS Act through rulemaking Recent opportunities to educate regulators include the FinCEN and OFAC jointly proposed rule implementing the GENIUS Act's AML and sanctions compliance requirements for permitted payment stablecoin issuers, with its open comment period having just ended in early June. The OCC completed the comment period for its proposed implementation of the GENIUS Act, in early May. As federal agencies propose additionalGENIUS Act rulemaking in the coming weeks, industry will have active opportunities to shape the frameworks that will govern privacy-preserving stablecoin infrastructure. These opportunities are time-limited, and the industry cannot afford to cede the conversation to parties less familiar with the technology's capabilities and constraints.[29]

B. What Regulators and Policymakers Must Do

The most immediate need is clarity. Regulators should provide explicit guidance on the permissibility of privacy-preserving technologies for regulated stablecoin issuers. The current silence on this question creates uncertainty that chills both investment in and adoption of compliant privacy solutions. Issuers and their technology partners need to know whether deploying on a privacy-preserving blockchain is compatible with their regulatory obligations—and the answer should be yes, provided appropriate mechanisms for regulatory access and audit are maintained.

The OCC's GENIUS Act rulemaking is the most immediate venue for this clarification. The final rule should establish that on-chain transaction data generated in connection with a customer relationship does not lose its protected status simply because it appears on a

[28]GENIUS Act § 3 (dual-track federal-state regulatory structure requiring "substantially similar" state frameworks).
[29]FinCEN and OFAC, Proposed Rule: Permitted Payment Stablecoin Issuer Anti-Money Laundering/Countering the Financing of Terrorism Program and Sanctions Compliance Program Requirements, Docket No. FINCEN-2026-0100, 91 Fed. Reg. 18,582 (Apr. 10, 2026) (comment period closed June 9, 2026), https://www.federalregister.gov/documents/2026/04/10/2026-06963/permitted-payment-stablecoin-issuer-anti-money-launderingcountering-the-financing-of-terrorism; OCC, Notice of Proposed Rulemaking, Implementing the Guiding and Establishing National Innovation for U.S. Stablecoins Act for the Issuance of Stablecoins, Docket ID OCC-2025-0372, 91 Fed. Reg. 10202 (Mar. 2, 2026) (comment period closed May 1, 2026), https://www.federalregister.gov/documents/2026/03/02/2026-04089/implementing-the-guiding-and-establishing-national-innovation-for-us-stablecoins-act-for-the.

public ledger. The proposed rule's treatment of distributed ledger data as "publicly available information" creates a compliance gap that the OCC should close—not codify.

More broadly, regulators should not equate privacy-seeking behavior with illicit intent. As Commissioner Peirce has argued, protecting one's financial privacy should be the norm, not an indicator of criminal intent. Regulators should also create safe-harbor or sandbox frameworks that allow regulated institutions to pilot privacy-preserving stablecoin solutions without facing enforcement risk for good-faith experimentation. The GENIUS Act's directive to FinCEN to facilitate novel detection methods provides a statutory basis for this kind of forward-looking regulatory approach.[30]

C. What Financial Institutions Must Do

Financial institutions that are evaluating stablecoin adoption for treasury, settlement, or payment operations should recognize that privacy infrastructure will be a prerequisite—not an optional feature. The time to begin evaluating privacy-preserving solutions is now, while implementing regulations are still being written and the competitive landscape for compliant privacy infrastructure is still forming.

Institutions will also need to build internal expertise at the intersection of blockchain technology, cryptography, and financial regulation. This is a new competency that existing compliance and technology teams will need to develop—through hiring, partnerships, and direct engagement with the developers building these systems.

V. Conclusion

The GENIUS Act is a landmark achievement in digital asset regulation. By establishing a comprehensive supervisory framework for payment stablecoins, it creates the conditions for institutional adoption at scale. But its success depends on solving the privacy problem it left unaddressed. A stablecoin regime built on transparent public blockchains will be structurally unable to comply with existing financial privacy law, commercially unattractive to the institutions it is meant to serve, and potentially corrosive to the civil liberties that American financial regulation has long sought to protect.

The regulatory signals are encouraging. The SEC, Treasury, and the White House have all indicated that privacy-preserving technology is compatible with—and necessary for—a well-functioning digital financial system. The technology to close the privacy gap exists today. What is needed now is coordinated action: from industry to build compliant solutions; from regulators to provide the clarity and frameworks that enable adoption; and from financial institutions to begin integrating privacy infrastructure into their operations. The window for shaping these outcomes is open, but it will not remain so indefinitely.

---

[30] Executive Order on Strengthening American Leadership in Digital Financial Technology, January 23, 2025. https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/

About the Georgetown Psaros Center for Financial Markets and Policy

The Georgetown Psaros Center for Financial Markets and Policy is the preeminent destination for unbiased expertise at the intersection of finance and policy. The Psaros Center provides thought leadership and actively contributes to shaping global finance. Located in Washington, D.C., we connect policymakers, industry leaders, and scholars through solutions-driven platforms.

Housed at Georgetown University's McDonough School of Business, the Psaros Center for Financial Markets and Policy serves as an impartial, academic-based research center. The Psaros Center integrates practice with policy: facilitating a forum for solutions-oriented discussion, conducting relevant and original research on key global market issues, and engaging students interested in the nexus of finance and policy. Collectively, our efforts impact policy and practice by informing current industry professionals, the next generation of finance and policy leaders, and the world, to create meaningful change.

Visit us at finpolicy.georgetown.edu.

About this Research: At the Georgetown Psaros Center for Financial Markets and Policy, we believe in fostering the next generation of financial leaders by providing our students with the unique opportunity to engage in high-level research alongside seasoned experts. This publication is a product of our collaborative research program, co-authored by our Visiting Fellows and talented Georgetown University students. While the center is pleased to facilitate this scholarly exchange, the perspectives expressed in this paper do not necessarily represent the views of the center, the McDonough School of Business, or Georgetown University.