HAYNES BOONE

FINANCIAL SERVICES

REGULATORY ROUNDUP | AUGUST 2025

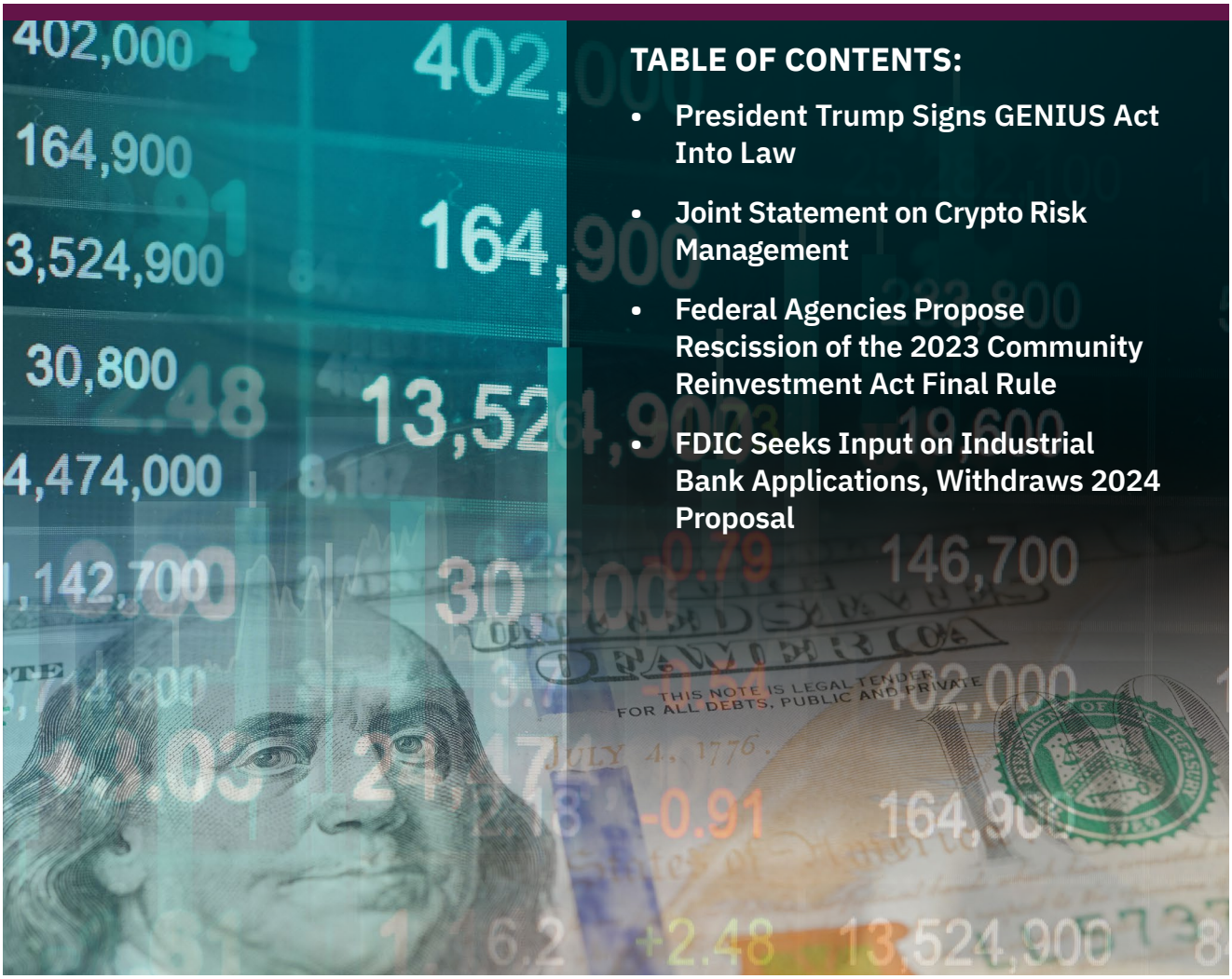


TABLE OF CONTENTS:

President Trump Signs GENIUS Act Into Law – Neil Issar, Leel Sinai

After extended congressional wrangling, President Donald Trump finally signed the Guiding and Establishing National Innovation for U.S. Stablecoins Act (the "GENIUS Act" or the "Act") into law on July 18, 2025. The Act establishes a comprehensive regulatory framework for the issuance of stablecoins to provide clarity to industry participants and promote consumer participation in the crypto marketplace. It takes effect 18 months after the date of enactment or 120 days after an agency finalizes regulations implementing the statute – whichever is earlier.

Scope of the Act

The GENIUS Act applies to "payment stablecoins," defined therein as digital assets (i.e., digital representations of value recorded on a cryptographically secured digital ledger) used or designed to be used as a means of payment (as opposed to an investment), and that can be exchanged or redeemed for a stable, fixed amount of monetary value (typically by being tied to a national currency such as the U.S. dollar).

“Once the Act becomes effective, only permitted stablecoin issuers will be able to issue payment stablecoins.”

The Act does not apply to digital assets that are themselves national currencies or deposits, those that are considered securities (regulated by the Securities and Exchange Commission) or commodities (regulated by the Commodity Futures Trading Commission), or that pay holders yield or interest solely for the holding, use or retention of the assets.

Likewise, the Act does not apply to direct transfers of digital assets between two individuals or entities without an intermediary, transfers of digital assets between an individual’s or entity’s account in the United States and the same individual’s or entity’s foreign account, and “any transaction by means of a software or hardware wallet that facilitates an individual’s [or entity’s] own custody of digital assets.”

Permitted Issuers of Stablecoins

Once the Act becomes effective, only permitted stablecoin issuers will be able to issue payment stablecoins. A permitted stablecoin issuer is a U.S. entity that is a subsidiary of any bank approved to issue stablecoins, or a federal- or state-qualified payment stablecoin issuer (discussed below). Generally, public companies that are not engaged in financial activities and foreign companies will not be able to issue payment stablecoins.

In addition to issuing payment stablecoins, permitted stablecoin issuers will also be able to redeem payment stablecoins; manage related reserves, including purchasing, selling, and holding reserve assets or providing custodial services for reserve assets; provide custodial or safekeeping services for payment stablecoins, required reserves or private keys of payment stablecoins; and undertake other activities that directly support any of the aforementioned activities.

Three years after the Act’s enactment (i.e., after July 18, 2028), digital asset service providers—entities that are in the business of exchanging, transferring, or storing digital assets or participating in financial services relating to digital asset issuance—will not be allowed to offer or sell stablecoins in the United States unless the stablecoin is issued by a permitted issuer.

Two-Track Regulatory Framework

Typically, the financial institutions covered by the Act would be subject to regulatory oversight by one or more of the federal banking regulators—namely, the Office of the Comptroller of the Currency (“OCC”), the Federal Reserve Board (“Federal Reserve”), the Federal Deposit Insurance Corporation (“FDIC”) and the National Credit Union Administration (“NCUA”)—depending on the type of institution. But the Act introduces a two-track regulatory framework that permits certain smaller issuers, those with less than $10 billion in outstanding stablecoins, to opt into a scheme of regulation by state agencies, provided that scheme is certified as “substantially similar” to the federal regulatory framework by a new Stablecoin Certification Review Committee, composed of the Department of the Treasury, the Federal Reserve and the FDIC.

"Violating the Act or failing to comply with its requirements can result in criminal, civil or regulatory penalties. For example, unlicensed stablecoin issuers can be charged up to $100,000 per day in civil penalties, and knowing violations may be subject to fines of up to $1 million per violation, imprisonment for up to five years or both."

The Act also imposes transition obligations. Once a state-certified issuer exceeds the $10 billion threshold, it must either transition to the federal regime within a year or obtain a waiver from federal regulators to remain under state supervision. This waiver may be granted based on factors such as the issuer's capitalization, regulatory history and the strength of the state framework.

Liquidity and Compliance Requirements for Issuers

Permitted stablecoin issuers must affirmatively comply with several requirements. For instance, they must maintain identifiable reserves backing outstanding stablecoins on a one-to-one basis. Reserves may be in the form of U.S. currency, Treasury bills, notes, or bonds, repurchase and reverse repurchase agreements, and other liquid, government-issued assets. Permitted issuers must file monthly reports regarding their reserve composition to be examined by third-party auditors. If a permitted issuer is not a public company and has more than $50 billion in outstanding stablecoins, then it must also provide annual audited financial statements, which will be both publicly available and filed with regulators.

Permitted issuers must also publicly disclose their redemption policies, including the redemption timeline and all fees. Moreover, they must comply with all applicable Bank Secrecy Act requirements for financial institutions, including those related to economic sanctions, anti-money laundering, customer identification and due diligence. These requirements may be modified by future regulatory guidance or rulemaking because, within three years of its enactment, the Act requires the Financial Crimes Enforcement Network to implement "innovative or novel methods, techniques, or strategies by regulated financial institutions to detect illicit activity involving digital assets" as well as standards for permitted stablecoin issuers to "identify and report illicit activity" involving stablecoins, including "fraud, cybercrime, money laundering, financing of terrorism, sanctions evasion, or insider trading."

Prohibition on Misrepresentation of Insurance Status

The Act prohibits permitted issuers from misrepresenting stablecoins' insurance status—namely, that stablecoins are not backed or guaranteed by the federal government and are not protected by deposit insurance from the FDIC or share insurance from the NCUA.

Priority of Holders' Claims in Bankruptcy

The Act reforms the standard order of creditor repayment in bankruptcies by clarifying that stablecoin holders' claims against the bankruptcy estate of a permitted stablecoin issuer will have "first priority over any other claim," even if the issuer's reserves are insufficient to pay all claims for outstanding stablecoins. It remains to be seen whether and how this will work in practice.

Consequences of Noncompliance

Violating the Act or failing to comply with its requirements can result in criminal, civil or regulatory penalties. For example, unlicensed stablecoin issuers can be charged up to $100,000 per day in civil penalties, and knowing violations may be subject to fines of up to $1 million per violation, imprisonment for up to five years or both.

The Future

Passage of the GENIUS Act could lead to increased payment-focused use of stablecoins and rapid development of applications and platforms that support stablecoins. But it remains to be seen how traditional finance industry participants will embrace the law and implement its requirements. In the meantime, the federal financial agencies will be tasked with the responsibility of implementing the GENIUS Act through regulation during a time in which budgets and human resources have been cut. Prospective industry participants, for their part, will need to ensure their own technology, operational resources and talent will be ready for the potential influx of business and compliance requirements.

Read the GENIUS Act **here**.

Joint Agency Statement on Risk Management Considerations for Banks Safekeeping Crypto-Assets – Neil Issar, Dustin Leenhouts

On July 14, 2025, three of the key federal bank regulatory agencies—the OCC, the Federal Reserve and the FDIC—issued a joint statement (the "Joint Statement") providing guidelines for banking organizations that provide, or are considering providing, safekeeping of crypto-assets. The Joint Statement does not create any new supervisory expectations but rather summarizes how existing laws, regulations and general risk management principles apply to the safekeeping of crypto-assets.

General Risk Management Considerations

The Joint Statement highlights several risk factors to be considered by banks prior to offering crypto-asset safekeeping:

1) The core financial risks given the strategic direction and business model
2) The ability to understand a complex, evolving and potentially unfamiliar asset class, including by keeping abreast of industry-leading practices
3) The ability to ensure a strong control environment
4) Contingency plans to address any unanticipated challenges in effectively providing services
5) The evolving nature of the industry and underlying technology
6) The potential need for significant resources and attention
7) The risk of price volatility

The Joint Statement also emphasized the importance of a bank's board, officers and employees having sufficient knowledge and understanding to establish adequate operational capacity and appropriate controls to, in turn, provide safekeeping services in a safe, sound and legally compliant manner.

Further, different products offer different regulatory and operational risks. As such, banks seeking to operate in this space should ensure they both understand the specifics of any product they wish to hold and implement a risk management system uniquely tailored to those products and their technical considerations as well as to different account models.

Cryptographic Key Management

The Joint Statement also provided a clear indication of potential legal liability with regard to holding crypto-assets. Banks that hold crypto directly control the underlying asset. End customers therefore lack the knowledge needed to transfer the underlying asset, meaning a bank could be liable for any losses the customer incurs due to fraud, unauthorized transfer or error on the part of the bank.

Banks that seek to operate in this space will need a robust risk management system for cryptographic keys and any other sensitive information used to control or transfer crypto-assets, including specific policies for lost or compromised keys. This includes an audit program that assesses cryptographic key generation, storage and deletion, controls related to transfer and settlement of customer assets, and the sufficiency of relevant information technology systems.

Legal, Compliance and Customer Risks

The Joint Statement also provided some clarity on the regulatory regimes with which banks must abide, including the Bank Secrecy Act, anti-money laundering laws, countering the financing of terrorism laws and rules promulgated by the Office of Foreign Assets Control.

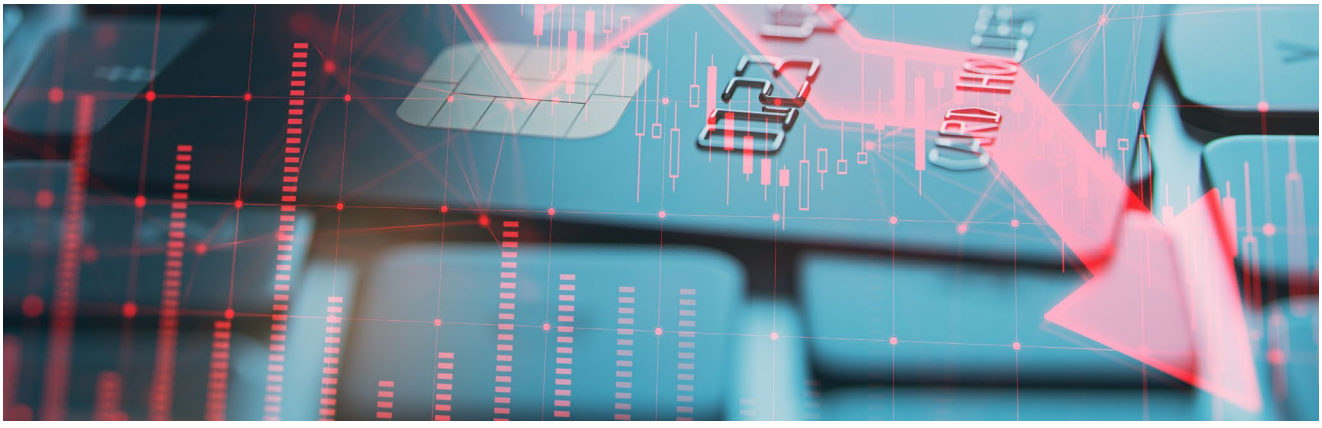
Moreover, it highlighted the need to ensure customers remain fully informed about a bank's role in any crypto-asset safekeeping activities, which may include ensuring a customer agreement and communications to customers clearly outlining the duties and responsibilities of the parties and address relevant safekeeping-specific issues (such as voting systems to manage and implement changes to crypto-asset blockchains, splitting or "forking" of an underlying cryptographic ledger, distributions of crypto-assets, the method in which crypto-assets are held and the use of smart contracts).

Third-Party Risk Management

The Joint Statement also discussed some of the unique considerations in cases where a bank employs a third-party sub-custodian or other service provider. Banks remain responsible for the activities performed by a sub-custodian, including the risk of lost or compromised keys. Due diligence before selection of a sub-custodian is therefore an important part of sound risk management. Such due diligence could include evaluating the effectiveness of the sub-custodian's key-management solution, including polices, processes and internal controls, as well as its adherence to standard safekeeping risk management practices.

The Joint Statement is the latest agency action intended to clarify and arguably promote digital asset-related activities by agency-supervised institutions.

Read the Joint Statement **here**.



“Vice Chair for Supervision Michelle W. Bowman stated, in support of the rescission, that the 2023 CRA Final Rule is “unnecessarily complex, overly prescriptive, and contained disproportionately greater costs than benefits,” echoing her dissenting statement regarding the 2023 CRA Final Rule in 2023.”

Federal Agencies Propose Rescission of the 2023 Community Reinvestment Act Final Rule – Leel Sinai, Tyler Sisca (Summer Associate)

On July 18, 2025, the OCC, the Federal Reserve and the FDIC (the “Agencies”) issued a joint notice of proposed rulemaking to rescind the Community Reinvestment Act (“CRA”) final rule issued in 2023 (the “CRA Final Rule”). Comments are due by Aug. 18, 2025.

The CRA was enacted in 1977 to encourage banks to help meet the credit needs of communities in which they were chartered. To achieve this, the CRA requires agencies to evaluate how banks meet the credit needs of their communities through performance tests and issue publicly available reports regarding reinvestment efforts.

The 2023 CRA Final Rule was issued on Oct. 24, 2023. The amendment included changes to the performance tests for different size banks, determined by asset-size thresholds that are updated yearly. Additionally, it updated regulations to account for internet and mobile banking. Although the rule would have become effective on April 1, 2024, most substantive provisions would only be applicable starting Jan. 1, 2026, or Jan. 1, 2027. During this transition period, the 1995 CRA regulations would apply. The April 1, 2024 effective date was later extended due to a preliminary injunction granted by the District Court for the Northern District of Texas on March 29, 2024. The Agencies later appealed and then filed a motion to stay the appeal, which was granted on April 1, 2025, pending the proposal to rescind the 2023 CRA Final Rule.

Vice Chair for Supervision Michelle W. Bowman stated, in support of the rescission, that the 2023 CRA Final Rule is “unnecessarily complex, overly prescriptive, and contained disproportionately greater costs than benefits,” echoing her dissenting statement regarding the 2023 CRA Final Rule in 2023.

In rescinding the 2023 CRA and issuing a new rule, the Agencies aim to (i) restore certainty in the CRA regulatory framework for stakeholders and (ii) limit the regulatory burden on banks. To achieve this, the new rule will (i) recodify the 1995 CRA regulations, (ii) amend the definition of “small bank” and add accompanying technical amendments, (iii) add technical amendments to the implementation of the CRA Sunshine Regulations of the Federal Deposit Insurance Act and (iv) add technical amendments to the Public Welfare Investments regulation. The notice explains that using the 1995 CRA regulations as the baseline would result in minimal costs to banks because those regulations are currently applicable. Additionally, this approach hopes to provide certainty in the near term, avoiding ongoing uncertainty caused by continued litigation.

Read the Proposal to Rescind **here**.

FDIC Seeks Input on Industrial Bank Applications, Withdraws 2024 Proposal – Leel Sinai

On July 15, the FDIC issued a request for information ("RFI") seeking public input on how it should evaluate statutory factors for industrial bank and industrial loan company ("ILC") applications. The RFI focuses on deposit insurance applications and related filings under the Bank Merger Act ("BMA") and Change in Bank Control Act ("CIBCA"). It invites feedback on the nature and structure of companies that have applied, or may apply, for an ILC charter and federal deposit insurance, or for approval or non-objection to enter into other corporate transactions involving industrial banks, and the issues those applications and notices may present. According to the FDIC, this process will inform potential changes to how the agency evaluates the statutory factors in the context of the unique aspects of industrial bank business plans and the issues presented by the range of companies that may form an industrial bank.

The FDIC is particularly interested in how to:

1) Apply the Federal Deposit Insurance ("FDI") Act's statutory factors to ILCs and whether they should be applied differently to industrial bank applicants than to other types of applicants

2) Tailor its evaluations based on the size, complexity, and nature of the parent and affiliates of a proposed industrial bank

3) Review applications where an affiliate of a proposed industrial bank already provides the same lending (or other) services the proposed industrial bank would provide to customers of the parent organization

4) Assess an industrial bank applicant's risk to the Deposit Insurance Fund, its capital adequacy, and the convenience and needs of a community to be served by an industrial bank applicant

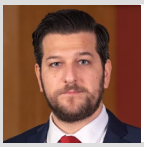
5) Consider other statutory factors under the BMA, CIBCA and FDI Act

Comments on the RFI will be due 60 days after it is published in the Federal Register.

The FDIC also withdrew its July 2024 proposal that would have created presumptions treating certain ILCs as shell or captive, which would weigh heavily against approval. The FDIC stated that it no longer intends to issue a final rule with respect to this proposal, but if it decides to make changes in this area, it will do so through future regulatory action. Acting Chairman Travis Hill emphasized that the FDIC's ultimate objective should be a policy statement or similar issuance that provides clarity on how the FDIC interprets the applicable statutory factors in the context of ILC filings. He also confirmed that, during the RFI process, the agency will continue work on pending ILC applications that have been filed with the agency.

Read the RFI and the withdrawal **here** and **here**.

EDITOR

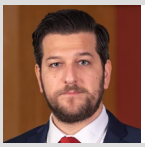


Leel Sinai
Leel.Sinai@haynesboone.com
T +1 212.835.4898

ISSUE CONTRIBUTORS

Dustin Leenhouts
Dustin.Leenhouts@haynesboone.com
T +1 214.651.5319

Neil Issar
Neil.Issar@haynesboone.com
T +1 214.651.5281



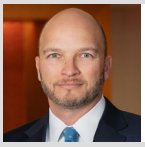
Leel Sinai
Leel.Sinai@haynesboone.com
T +1 212.835.4898

Tyler Sisca - Summer Associate
Click here to view Tyler's LinkedIn profile

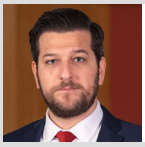
FINANCIAL REGULATORY CONTACTS

Giorgio Bovenzi
Giorgio.Bovenzi@haynesboone.com
T +1 212.918.8998

Matthew Frankle
Matthew.Frankle@haynesboone.com
T +1 212.918.8950



Alex Grishman
Alexander.Grishman@haynesboone.com
T +1 212.918.8965



Leel Sinai
Leel.Sinai@haynesboone.com
T +1 212.835.4898

Brian Sung
Brian.Sung@haynesboone.com
T +1 212.659.4964

Craig Unterberg
Craig.Unterberg@haynesboone.com
T +1 212.659.4987

haynesboone.com

For a complete list of our Financial Regulatory newsletters, please click **here**.

Sign up to receive our newsletter by clicking **here** and selecting the **Financial Regulatory** list