HAYNES BOONE

# FINANCIAL SERVICES

## REGULATORY ROUNDUP | SEPTEMBER 2025

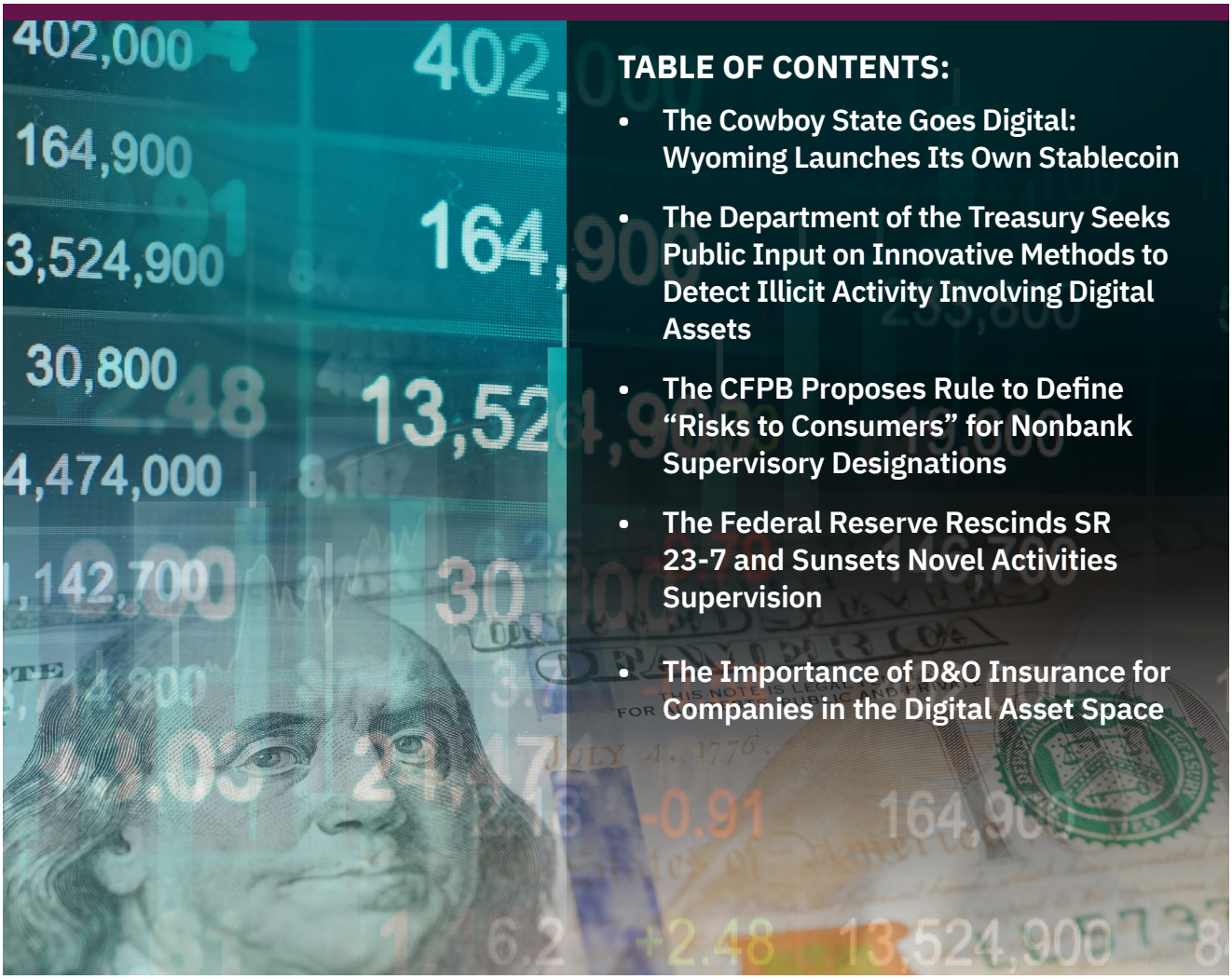


**TABLE OF CONTENTS:**



### The Cowboy State Goes Digital: Wyoming Launches Its Own Stablecoin – Leel Sinai, Dustin Leenhouts

On Aug. 29, 2025, Wyoming officially launched its own stablecoin, making it the first public entity to issue a stable coin in the United States. The stablecoin, named the Frontier Stable Token ("FRNT"), will be held and managed by the Wyoming Stable Token Commission (the "Commission"), created in March 2023. The Commission will hold dollars and short-duration treasuries in reserve to ensure the coin maintains a consistent value. The Commission also stated it would conduct regular audits and uphold strict standards for safeguarding and managing the reserve assets.

**Purported Benefits**

In a brief produced by the Commission in May, the Commission highlighted the benefits of the newly minted coin: transparency, reduced transaction costs and instant payments. It also highlighted that any investment income produced by the project would support the Wyoming public school fund. In a press release about the issuance, the chairman of the Commission, Wyoming Governor Mark Gordon, said FRNT is intended to empower Wyoming residents and businesses to transact in the digital age.

**“While FRNT was officially launched the week of Aug. 25, 2025, the ability to buy and sell the coin will be restricted for the coming days to weeks.”**


**National Fight**

This announcement comes on the heels of a national fight about the role of government in the future of the crypto market. Republican Senator Ted Cruz recently introduced the Anti-CBDC Surveillance State Act in the Senate, arguing that government-issued stable coins are a sign of government overreach and will lead to increased national spying. Previous legislative efforts have indicated that some Democratic lawmakers are open to a stablecoin issued by the Federal Reserve. For example, the Central Bank Digital Currency Study Act of 2021 required the central bank to study the impact of the introduction of a central bank backed digital currency.

**Next Steps**

While FRNT was officially launched the week of Aug. 25, 2025, the ability to buy and sell the coin will be restricted for the coming days to weeks. The Commission is working closely with Wyoming-domiciled crypto exchange Kraken to roll out public trading.

Read the Wyoming Stable Token Brief **here**.

Read Governor Mark Gordon’s Press Release **here**.

## The Department of the Treasury Seeks Public Input on Innovative Methods to Detect Illicit Activity Involving Digital Assets – Neil Issar

On Aug. 18, 2025, the U.S. Department of the Treasury (the “Treasury”) issued a Request for Comment (the “Request”) seeking public input on innovative or novel methods, techniques or strategies that financial institutions currently use, or could potentially use, to detect illicit activity and mitigate illicit finance risks involving digital assets. The Request is a required initiative under the recently enacted Guiding and Establishing National Innovation for U.S. Stablecoins (“GENIUS”) Act. It also aligns with Executive Order 14178, which seeks to establish regulatory clarity for and promote innovation of digital financial technology.

The Request invites public comment on a list of questions, with a focus on innovative or novel methods, techniques or strategies related to four subjects:

1. Application Program Interfaces (“APIs”): With APIs being critical in enabling secure, automated and real-time data sharing between software applications, the Treasury is interested in how they can be used to facilitate compliance with anti-money laundering (“AML”) and countering the financing of terrorism (“CFT”) requirements as well as to monitor and access transaction data.

2. Artificial Intelligence (“AI”): The Request seeks information on the use of AI to analyze large volumes of transactional data, identify complex illicit financial networks and detect patterns indicative of money laundering or other illegal activities. The Treasury is particularly interested in the benefits, challenges and risks associated with deploying AI for AML/CFT compliance, including issues related to model accuracy, interpretability and operational feasibility.

**“The Treasury is interested in how these technologies can enhance the detection of illicit activities within the digital asset ecosystem, such as money laundering, ransomware attacks, fraud, terrorist financing and sanctions evasion.”**

3. Digital Identity Verification: The Treasury is exploring how portable digital identity credentials—potentially incorporating government-issued IDs or biometrics—can streamline onboarding, support AML/CFT compliance and protect user privacy. The Request also considers the application of digital identity tools in decentralized finance environments, such as automated checks in smart contracts.

4. Blockchain Technology and Monitoring: The Treasury seeks input on how blockchain technology can be used to trace transactions, identify links to known illicit addresses (e.g., darknet markets, sanctioned entities) and comply with AML/CFT requirements. Despite the proliferation of crypto and blockchain technology in the financial sector, integrating such technology with legacy banking systems while addressing fund-origin-masking services like mixers still poses a number of technical and logistical challenges.

In short, the Treasury is interested in how these technologies can enhance the detection of illicit activities within the digital asset ecosystem, such as money laundering, ransomware attacks, fraud, terrorist financing and sanctions evasion.

For each method, technique or strategy discussed, the Treasury requests feedback on several research factors, including:

- Improvements in the ability to detect illicit activity
- Associated costs and resource burdens
- Volume and sensitivity of data collected
- Privacy and data protection risks
- Operational and efficiency challenges
- Cybersecurity vulnerabilities
- Overall effectiveness in mitigating illicit finance risks

The Request is directed at a broad range of stakeholders, including financial institutions, technology providers, industry experts and the general public. All comments will be publicly viewable and stakeholders are encouraged to provide detailed, data-driven input on the effectiveness, risks and implementation challenges of the technologies under consideration. Additionally, the feedback collected will inform the Treasury's future research and policy recommendations, with the goal of developing a robust regulatory framework that balances innovation with effective AML/CFT compliance and crime prevention. Ultimately, the Treasury's stated aim is to issue guidance and propose rulemaking that supports the use of digital assets, particularly in the context of stablecoins and decentralized finance, while safeguarding the nation's financial system from illicit activities. The public comment period is open until Oct. 17, 2025.

Read the Request **here**.

### The CFPB Proposes Rule to Define "Risks to Consumers" for Nonbank Supervisory Designations – Leel Sinai

On Aug. 26, 2025, the Consumer Financial Protection Bureau ("CFPB") issued a proposed rule that would, for the first time, establish a binding standard for determining when a nonbank financial firm may be subject to CFPB supervision under Section 1024(a)(1)(C) of the Consumer Financial Protection Act ("CFPA").

The CFPA authorizes the CFPB to supervise a nonbank covered person if it has "reasonable cause to determine" that the entity is engaging in conduct posing "risks to consumers" in connection with consumer financial products or services. While the CFPB has long had procedures governing designation proceedings under 12 CFR part 1091, it has never defined what constitutes "risks to consumers." Instead, it has proceeded through case-by-case adjudication.

**“The CFPB proposes to define conduct posing “risks to consumers” as conduct that: (a) presents a high likelihood of significant harm to consumers; and (b) is directly connected to the offering or provision of a statutorily defined consumer financial product or service.”**

According to the CFPB, this ad hoc approach creates three problems: (1) inconsistent application of the standard across orders; (2) uncertainty for firms about what conduct may trigger designation; and (3) risk that the CFPB may not adhere to the best reading of its statutory authority. The proposed rule seeks to resolve these concerns by adopting a uniform legal standard.

**Elements of the Proposal**

The CFPB proposes to define conduct posing “risks to consumers” as conduct that: (a) presents a high likelihood of significant harm to consumers; and (b) is directly connected to the offering or provision of a statutorily defined consumer financial product or service.

The CFPB explains that Congress likely did not intend for supervisory resources to be spent on speculative or trivial harms. Earlier CFPB orders sometimes applied the phrase broadly to encompass immaterial risks. Under the proposal, only serious, consumer-impacting conduct would qualify.

The CFPB also emphasizes that the “direct connection” requirement ensures it will focus only on products and services explicitly covered under the CFPA, rather than tangential activities. The CFPB is also soliciting comment on whether “risks to consumers” should be limited to potential violations of law.

**Potential Impacts**

The CFPB expects fewer nonbanks will be designated for supervision under the narrower standard. Firms may also benefit from clearer guidance on what conduct could trigger oversight, potentially lowering compliance review costs. Some firms may feel freer to engage in conduct that poses some chance of harm but not a “high likelihood of significant harm,” potentially shifting compliance strategies.

This proposed rule provides welcome clarity for nonbank financial services providers. Firms engaged in lending, payments, debt collection, credit reporting and other covered activities should review their compliance frameworks in light of the CFPB’s narrower focus on serious and directly connected consumer harms. While the immediate supervisory footprint may shrink, the rule underscores the CFPB’s intent to concentrate its resources on conduct with meaningful consumer impact.

Comments are due 30 days after publication in the Federal Register. The final rule would take effect 30 days after publication, unless determined to be a “major rule,” in which case the effective date would be 60 days.

Read the Proposed Rule **here**.

## The Federal Reserve Rescinds SR 23-7 and Sunsets Novel Activities Supervision – Leel Sinai

The Federal Reserve Board (the "Federal Reserve") announced on Aug. 15, 2025, that it has rescinded SR 23-7, the supervisory letter that established its Novel Activities Supervision Program ("NASP"). The move formally ends the Federal Reserve's stand-alone oversight program for cryptoasset activities, distributed ledger technology ("DLT") and certain complex bank–fintech partnerships. Going forward, novel activities will be monitored through the Federal Reserve's traditional supervisory framework rather than a dedicated program.

### Background: What SR 23-7 Did

On Aug. 8, 2023, the Federal Reserve issued SR 23-7, creating NASP to provide enhanced oversight of state member banks engaging in activities viewed as novel or higher risk. These included:

- Custody, trading, or other services related to crypto assets
- Use of distributed ledger technology to deliver financial products or services
- Complex partnerships between banks and nonbanks to deliver consumer financial products, often through digital platforms

NASP supplemented ordinary safety and soundness supervision with horizontal reviews, continuous data monitoring and targeted exams. The Federal Reserve's stated aim was to deepen its understanding of emerging technologies and the risk management practices needed to oversee them effectively.

### Why the Federal Reserve Withdrew SR 23-7

In its release, the Federal Reserve explained that after two years of supervisory work, it had "strengthened its understanding" of novel activities and related risk management. The Federal Reserve determined that oversight could be fully integrated into the routine supervisory process, eliminating the need for a stand-alone program.

The withdrawal of SR 23-7 follows an earlier step on Apr. 24, 2025, when the Federal Reserve rescinded SR 23-8 / CA 23-5, which required banks to seek supervisory non-objection before engaging in certain stablecoin and dollar-token activities. At the same time, the Federal Reserve also withdrew some 2022 digital-asset guidance. Together, these actions mark a broader shift back to baseline supervision of novel activities.

### Implications for Banks and Fintech Partnerships

Novel activity supervision will now occur through regular exam cycles, CAMELS ratings, and consumer compliance reviews. Banks should expect their lead supervisory team to scope and address these risks in the ordinary course. Moreover, the rescission does not lessen regulatory expectations. Banks must continue to demonstrate strong board oversight, robust vendor due diligence, well-developed capital and liquidity planning, and effective compliance with BSA/AML and consumer protection requirements.

**"The Federal Reserve determined that oversight could be fully integrated into the routine supervisory process, eliminating the need for a stand-alone program."**

By embedding novel activities into its standard processes, the Federal Reserve signals it no longer sees them as categorically exceptional, but rather as another dimension of risk management. Banks engaging in crypto-related services or fintech partnerships should not scale back controls. Instead, they should be prepared to evidence sound governance and consumer safeguards during routine exams.

**Takeaways**

The Federal Reserve's decision to withdraw SR 23-7 reflects growing supervisory familiarity with crypto and fintech activities. For banks, the change may reduce the sense of "exception-based" oversight, but it does not diminish regulatory scrutiny. Instead, it underscores that novel activities are now firmly part of the mainstream supervisory agenda.

Read the Press Release **here**.

## The Importance of D&O Insurance for Companies in the Digital Asset Space – Peter A. Halprin, Brian Sung, and Keeton Field (Summer Associate)

***This article was first published online by the American Bar Association.***

Although a broad ecosystem has long existed in the digital assets community (including crypto-native platforms such as centralized exchanges, liquidity providers, lending platforms, custodians and other service providers, and retail investors, high net worth "whales" acting as both venture/seed investors and platform founders, and (in recent years) exchange traded funds and digital asset hedge funds), the sector is now experiencing a rapid increase in new entrants, such as digital asset treasury companies and other traditional businesses holding bitcoin and other digital assets on their balance sheets.[1]

Some of these holders have an explicit strategy or mandate to acquire and accumulate bitcoin or other digital assets as a primary objective (as well as crypto-adjacent firms such as bitcoin miners, exchanges, fintech payment processors and other service providers, whose holdings are naturally aligned with their businesses). However, a growing number of unrelated businesses are now also continuing to pursue their primary activities while adding bitcoin or other digital asset exposures, either to diversify corporate treasury assets or as an ancillary investment, hedging or other strategic initiative. This includes, for example, household names such as Tesla and GameStop, but also some lesser-known entities such as the coal producer Alliance Resource Partners, the video-sharing and cloud services platform Rumble, and the design software firm Figma.

These holders may also employ leverage, complex capital structure arbitrage, derivative instruments, private investments in public equity special purpose acquisition company (and other complex financing techniques) to facilitate and execute their digital asset accumulation strategies. Such entrants include both private and public listed companies with a range of stakeholders, such as preferred share, convertible debt, warrant and common equity holders. They interface with a variety of transactional partners, some of which are arms' length counterparties (or even those with no direct privity such as traders of options on the firms' securities), but some of which may be secured creditors holding liens on the firms' assets.

After an extended period of "crypto winter" following the digital assets market downturn in 2021–22, and a relatively challenging regulatory environment in the U.S. under the Biden administration, the outlook for the digital assets market and interest in platforms and tokens have seen a strong resurgence over the past year, aided in part by a more innovation-focused and constructive regulatory approach. The regulatory picture continues to evolve rapidly. For example, in July 2025, the GENIUS (Guiding and Establishing National Innovation for U.S. Stablecoins) Act was passed and signed into law, establishing a comprehensive federal framework for payment stablecoins. Additional proposed legislation addressing market structure and clear allocation of authority among regulators remains under consideration. The House passed the Digital Asset Market Structure Clarity Act of 2025 in July 2025. The Senate is considering a draft of a Responsible Financial Innovation Act of 2025, intended to address oversight of digital asset securities, and a potential future bill to cover oversight of digital asset commodities. The Securities and Exchange Commission, the Commodity Futures Trading Commission and the White House also have expressed intent to move quickly to implement additional guidance and regulatory clarity.

Holding digital assets on corporate balance sheets has also become more tenable for public companies in light of updated accounting guidance that now permits the fair-value accounting and timely recognition of both gains and losses on digital assets. The previous "impairment" model required recognition of unrealized losses but not unrealized gains.[2]

Against the backdrop of this regulatory thaw is an environment ripe for not only a new era of digital assets innovation, but also for high-profile and high-stakes litigation against companies in the digital asset space. While the crypto market has been no stranger to litigation, regulatory investigations or enforcement actions, it is foreseeable that the increased participation by more traditional types of corporate entities with new classes of investors and stakeholders may give rise to new types of potential claims or causes of action in the event of disputes or (alleged or actual) misfeasance. Plaintiffs may also find newly capitalized, high-profile crypto firms to be more attractive targets for existing claims they might not have pursued against the legacy businesses. At the same time, reduced emphasis on enforcement and oversight may open the door to more bad actors seizing the opportunity to engage in criminal, fraudulent or manipulative activity. According to one recent analysis, legal experts are forecasting a rise in civil litigation in crypto due to the "perfect storm" of increased investment and decreased enforcement.[3]

**Lawsuits Coming**

The stage seems set for a wave of lawsuits, particularly around claims of fraud, misrepresentation, and asset recovery, or shareholder claims regarding securities law or other regulatory violations.

For example, just a few weeks before the passage of the GENIUS Act, a class action lawsuit[4] was filed against Strategy Incorporated (formerly known as MicroStrategy Incorporated) and certain of its officers in the U.S. District Court for the Eastern District of Virginia. The complaint alleges that the company and its officers made materially false and misleading statements regarding the company's business, operations, and prospects, the anticipated profitability of its bitcoin-focused investment strategy and treasury operations, the various associated risks and the magnitude of potential losses, and the financial impact of adopting fair value accounting standards, and seeks recovery for losses to investors in the company's securities, allegedly caused by the company's violations of federal securities laws.

Strategy Incorporated and its board also face a second[5] class action lawsuit alleging an invalid amendment to terms of its Perpetual Strike Preferred Stock without required authorization from common

stockholders. Other companies have faced claims from investors seeking rescission or damages arising from alleged failures to comply with various registration, licensing or other compliance requirements, which pattern seems likely to continue. While a number of lines of coverage can and will come into play to address risks arising in the digital assets space (see author's post on Considerations for Insuring Crypto Assets), the likelihood of focus on securities litigation and claims encourages consideration of directors' and officers' (D&O) insurance coverage.

## D&O Insurance Can Help to Protect Companies in the Digital Asset Space

D&O insurance typically protects "directors and officers in the event they are accused of wrongdoing in the performance of their management duties."[6] D&O insurance can also protect companies, including in connection with claims in relation to offerings or representations about securities. Although such coverage and awareness of such risks have been well established in other industries, the recent growing adoption of the digital asset treasury strategy has led to increased use of listed and private corporate entities with acquisition and holding of volatile digital assets as a primary or at least significant business objective. This has exposed a new set of directors and officers to such potential claims or actions, often from new classes of investors and stakeholders, who may in turn have access to remedies and causes of action that may not be as familiar to crypto-native investors, founders, or executives.

It is Important to note that D&O coverage may contain hurdles to coverage for parties In the digital assets sector. As a threshold matter, since D&O coverage tends to be claims-made, it is important to ensure that the claims covered under a policy dovetail with and are tailored to each digital asset company's idiosyncratic mix of liability risks, whether they are primarily civil or regulatory in nature. Indeed, given potential regulatory scrutiny and the complexity of the subject matter, digital asset companies should consider seeking coverage that includes costs of requests for information, subpoenas, and, more broadly, investigations, and potentially significant costs of expert witnesses or financial or market analyses that may be required in the event of litigation or disputes.

Likewise, broad governmental or regulatory exclusions could be highly detrimental to the utility of D&O coverage to a digital asset company. In the same way, exclusions involving cyber risk, digital asset theft, initial coin or similar offerings, or fluctuations in the value of virtual currency should be narrowed or removed, as appropriate. In addition, as with all D&O offerings, including those outside of the digital asset space, it is important that criminal or fraudulent conduct exclusions be severable and limited to those instances where there has been a final, non-appealable adjudication against the insured.

Definitions should be closely scrutinized and matched up with the potential risks to the company. For example, companies should look for broad definitions of "loss" or "damages," depending on the operative wording of the policy, to encompass all the potential remedies that plaintiffs' lawyers might seek.

Like definitions, conditions may also be particularly important for digital asset companies. As an example, albeit in a different risk area, when evaluating a crime policy for digital assets, we noticed that the operative valuation provision did not dovetail with the valuation provision in the client's customer contracts. Had it not been identified, such discrepancies and the gap in coverage could have resulted in the company's insurance covering substantially smaller "losses" than those actually suffered by the company.

## Looking Ahead

As crypto litigation continues to surge and the market for such coverage continues to expand and mature, insurers will likely refine their offerings—and exclusions.[7] Policyholders should stay proactive, not only in managing risk but also in seeking out coverage that reflects the evolving realities of the digital assets economy and each company's particular risks and exposures.

[1] *See* Will Owens, The Rise of Digital Asset Treasury Companies (DATCOs), Galaxy, July 30, 2025.

[2] *See* Financial Accounting Standards Board (FASB), Accounting Standards Update No. 2023-08 (December 2023) (Intangibles— Goodwill and Other—Crypto Assets (Subtopic 350-60)); Josef Rashty, FASB's New Guidance on Accounting for Crypto Assets, The CPA Journal (December 2024).

[3] *See* Michael A. Mora, 'Perfect Storm:' Crypto Litigation Surging, Law.com (July 7, 2025).

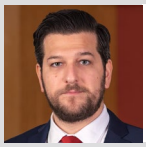
[4] Available at https://www.law360.com/articles/2355661/microstrategy-brass-face-suit-over-5-9b-bitcoin-loss.

[5] *See* https://www.sec.gov/Archives/edgar/data/1050446/000119312525163041/d94615d8k.htm.

[6] *See* Blockchain Technology and Digital Assets: Top 10 Reasons Why Insurance Matters, Marsh & McLennan Companies (2019).

[7] Kevin M. LaCroix, Crypto-Verse D&O Opportunity | The D&O Diary (July 16, 2025).

## EDITOR



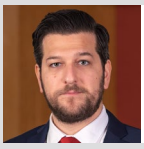
**Leel Sinai**
Leel.Sinai@haynesboone.com
T +1 212.835.4898

## ISSUE CONTRIBUTORS

**Peter A. Halprin**
Peter.Halprin@haynesboone.com
T +1 212.835.4878

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

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



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

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

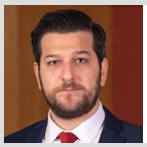
**Keeton Field** - Summer Associate
Click here to view Field's LinkedIn profile

## 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