

# Ten Key Regulatory Challenges of 2026

Balancing the Regulatory Stack

# Contents

<u>Introduction</u>	3	<u>08 Driving Capital Formation &amp; Growth</u>	41
<u>01 Executing Mandates</u>	4	<u>09 Expanding Digital Assets</u>	48
<u>02 Adopting Disruptive Tech &amp; AI</u>	9	<u>10 Enhancing Parties &amp; Workforce</u>	54
<u>03 Maintaining Cyber &amp; Data Security</u>	14	<u>KPMG Regulatory Insights</u>	60
<u>04 Mitigating Financial Crimes</u>	20	<u>Regulatory Analytics</u>	61
<u>05 Averting Fraud &amp; Scams</u>	25	<u>List of Acronyms</u>	62
<u>06 Protecting Fairness</u>	30	<u>List of Executive Orders</u>	64
<u>07 Ensuring Resiliency</u>	36		



# Introduction

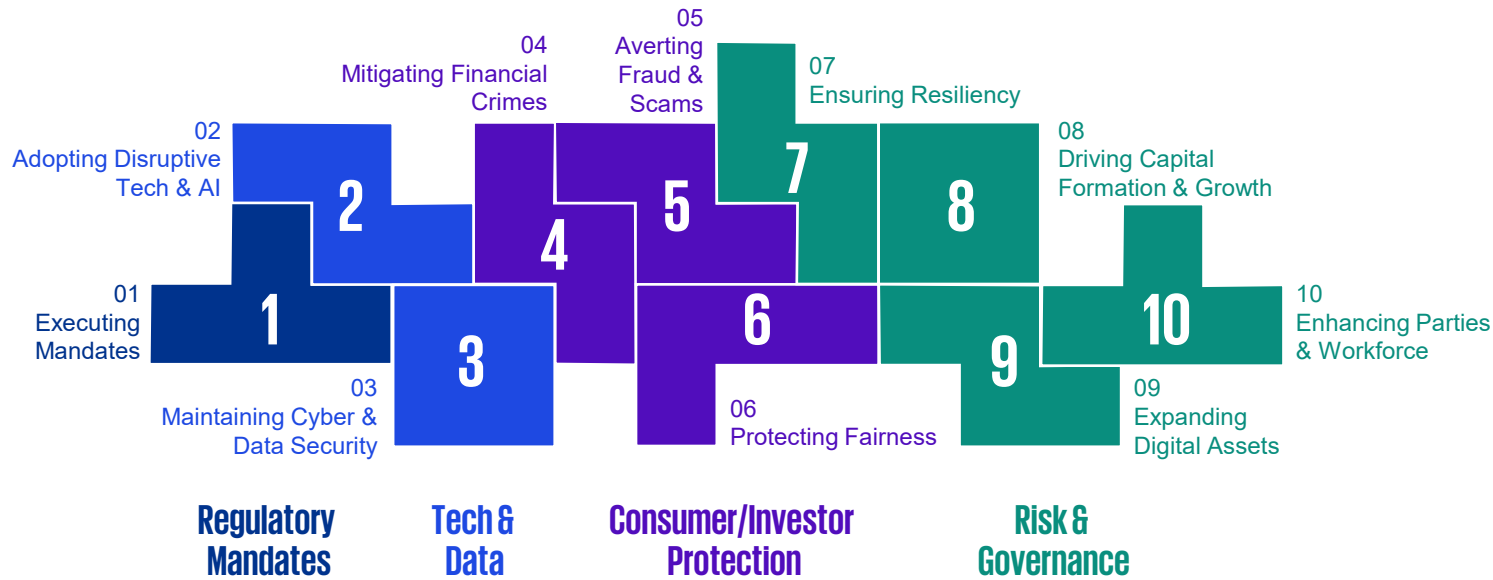
On behalf of KPMG Regulatory Insights, I am excited to issue our Ten Key Regulatory Challenges for 2026.

As we enter 2026, the regulatory landscape is being shaped by rapid technological innovation and evolving supervisory priorities. Recalibration of the many layers of policy, guidance and oversight that direct regulatory risk management and compliance is in process, in many cases effecting a “back-to-basics” approach.

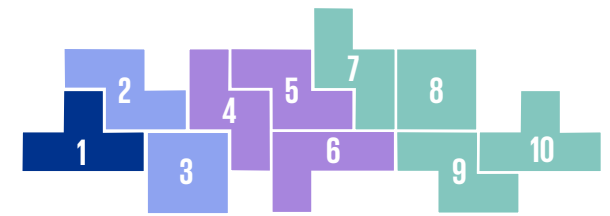
Organizations face a complex “regulatory stack” — requiring balance between innovation and control, speed and resilience, and modernization and stability.

In the following pages we project “what to watch” across ten key challenges based on regulatory signals observed in 2025. For all organizations, the overarching challenge will be **balancing the regulatory stack**.

**Laura Byerly**  
Managing Director  
Regulatory Insights



# 01 Executing Mandates



## Regulatory Signals

- Core Mission
- “Self-Regulation”
- Regulatory Divergence

*Aligning with the Administration’s priorities to reduce complexity, encourage innovation, and promote growth, regulators have narrowed supervision and enforcement to core statutory authorities; organizations must be cognizant of maintaining compliance with existing laws and regulations and growing regulatory divergence.*

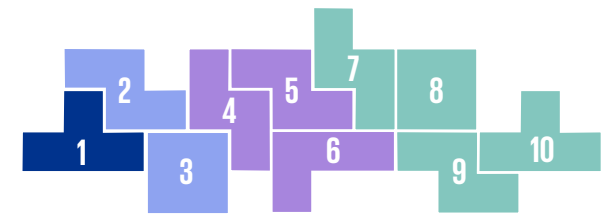
*“As the U.S. regulatory landscape evolves, regulators appear to be returning to fundamentals—core missions, statutory mandates—even as they embrace implementation of the digital financial technologies, like digital assets and AI applications, that are reshaping the financial system. This approach may signal a lighter supervisory touch in some areas and a growing reliance on market-driven discipline. For all organizations, the overarching challenge in 2026 will be to balance the regulatory stack.”*



**Laura Byerly**  
Managing Director  
Regulatory Insights



# 01 Executing Mandates



## Regulatory Signals

- Core Mission
- “Self-Regulation”
- Regulatory Divergence

### Signal

Federal agencies have focused resources on supervising and enforcing regulations based on their statutory authorizations, and in a manner consistent with the Administration’s priorities of reducing complexity, encouraging innovation, and promoting economic growth. Related actions include modified enforcement focus, rule rescissions/withdrawals, and cross-agency coordination.

### Examples

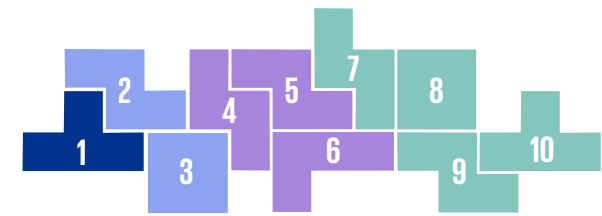
- Reviewing regulations for consistency with the law (e.g., EO 14219, Presidential Memo directing repeal of regulations)
- Publicly stating a return to “core mission” (e.g., agency statements SEC (Atkins, Pierce), EPA (Zeldin); FTC Draft Strategic Plan)
- Cross-agency identification of regulations that may hinder competition, entrepreneurship, and innovation (e.g., FTC/DOJ joint letter, anti-competitive task forces; FTC RFI)
- Efforts to harmonize regulatory requirements between agencies (e.g., SEC/CFTC roundtables on digital assets, prediction markets; ONCD efforts to coordinate cybersecurity requirements)
- Streamlining regulatory reviews and focusing on tailoring and reforming supervision processes (e.g., FRB, FDIC, OCC efforts to tailor requirements for large banks and community banks)

### What to Watch

- A “back-to-basics” approach to supervision and enforcement
- Ongoing tailoring of regulations based on size, scale, and risk profile
- Increasing use of guidance (e.g., FAQs) and frameworks



# 01 Executing Mandates



## Regulatory Signals

- Core Mission
- “Self-Regulation”
- Regulatory Divergence

### Signal

Through the withdrawal/recission of regulations, narrowed enforcement priorities, and increased reliance on guidance, regulators are exercising a “lighter touch” with regard to supervision and enforcement while simultaneously encouraging/incentivizing companies to identify, mitigate, remediate, and self-report misconduct.

### Examples

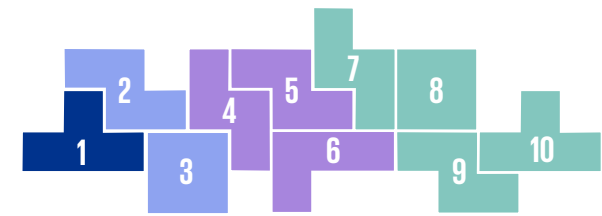
- Promotion of self-reporting, cooperation, and remediation (e.g., DOJ Criminal Division policies (white collar crime, crediting penalties); CFTC Enforcement Advisory)
- Focusing banking supervision on material risks (e.g., FRB, FDIC, OCC interagency proposed rule)

### What to Watch

- In the absence of regulation by enforcement, market-driven pressures will likely challenge companies to maintain their compliance and risk programs – “compliance is good for business”
- Long-standing regulations remain in place and still apply despite a shifting regulatory landscape. Board buy-in and investment in compliance will remain crucial to the success of the business



# 01 Executing Mandates



## Regulatory Signals

- Core Mission
- “Self-Regulation”
- Regulatory Divergence

### Signal

The regulatory landscape continues to grow in complexity as federal and state laws and regulations diverge due to differences in supervisory and enforcement priorities. In many instances, state activity (e.g., legislative, regulatory, enforcement) has increased to fill perceived gaps at the federal level (e.g., consumer/investor protections, data privacy, AI, climate/sustainability). Differences in global regulations and supervisory frameworks create divergent requirements by geography or jurisdiction.

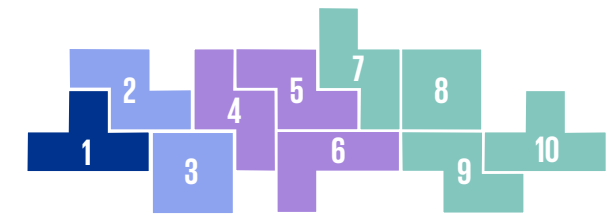
### Examples

- Recission of federal rules related to climate, DEI, fossil fuels (e.g., EO 14151, EO 14154, EPA rule withdrawals, SEC withdrawal of climate disclosure rule defense)
- State laws governing climate/sustainability (e.g., CA Corporate Climate Accountability Disclosure Act) and federal opposition (e.g., EO 14260)
- Identification and potential withdrawal/recission of federal rules perceived to inhibit AI innovation (e.g., OSTP RFI)
- Ongoing compliance requirements with global regulations (e.g., GDPR, DORA, EU AI Act, Paris Agreement)

### What to Watch

- Continuation and expansion of divergences between federal, state and global regulations and frameworks in certain areas including AI, digital assets, data privacy, and sustainability
- Rapid growth in regulatory changes across jurisdictions, including new wide-ranging “comprehensive” state AI laws
- Interagency coordination for U.S. revision of Basel III Endgame
- Potential streamlining of international laws and regulations

# 01 Executing Mandates



## Regulatory Signals

- Core Mission
- “Self-Regulation”
- Regulatory Divergence

## Relevant Thought Leadership



[Regulatory Alerts:  
State Series](#)



[First 100 Days:  
Regulatory Signals](#)



[Risk, Regulatory  
and Compliance](#)

## Top Related Regulatory Challenges

[02 Adopting Disruptive Tech & AI](#)

[03 Maintaining Cyber & Data Security](#)

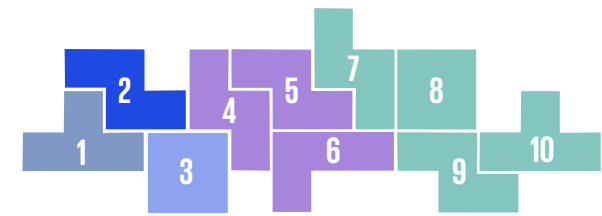
[08 Driving Capital Formation & Growth](#)

[09 Expanding Digital Assets](#)

[10 Enhancing Parties & Workforce](#)



# 02 Adopting Disruptive Tech & AI



## Regulatory Signals

- Model Risk Management
- Complexity & Divergence
- Public Private Partnership

*Federal and state regulatory adaptation of existing risk frameworks and policies respond to complexities in evolving AI innovation, with increasing private sector participation.*

*“Embracing AI in banking levels the playing field and provides unparalleled opportunity to enhance efficiency and optimization. Innovation and regulatory guidance must align to maintain compliance and consumer trust. By doing so, we foster a future of compliance and growth that benefits everyone.”*



**Adam Levy**  
Principal  
Advisory

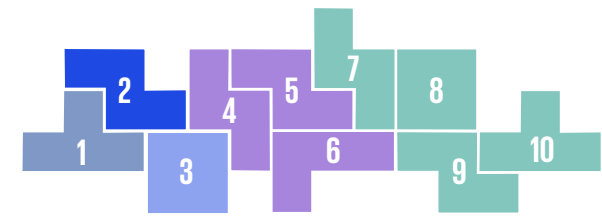
*“As regulations across the US continue to evolve and take shape in 2026, we expect a key focus area for organizations will be ensuring they have mechanisms in place to classify and validate that AI systems and guardrails are functioning as intended and are aligned with the regulations. As a result, we expect to see an uptick in the number of organizations conducting AI risk assessments, system testing, and other AI assurance activities in 2026.”*



**Bryan McGowan**  
Principal  
Advisory



# 02 Adopting Disruptive Tech & AI



## Regulatory Signals

- **Model Risk Management**
- Complexity & Divergence
- Public Private Partnership

### Signal

Federal banking regulators continue to reiterate that existing guidance and risk frameworks (e.g., SR 11-7 and OCC 2011-12) remain fit for purpose in supervising AI applications, but recent statements suggest some revisions may be needed as AI applications continue to evolve and are deployed across financial organizations.

### Examples

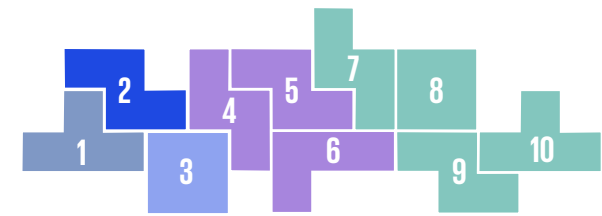
- Interagency belief that existing statutory authorities are generally sufficient to supervise AI use (e.g., GAO Report)
- If AI is a model, the current approach to model risk management needs to be revamped/revised (e.g., OCC Statement (Gould))
- Need to review/update existing standards (e.g., FRB Statement (Barr))

### What to Watch

- Potential revisions to existing model guidance for AI-specific use cases
- Potential need for enhancements to non-model risk frameworks to address transverse risks, including cybersecurity and operational risks, related to GenAI
- Increasing numbers of bank/fintech relationships; heightened attention to TPRM
- Growing acceptance that not all AI is a model
- Consideration of new approaches for AI that is not a model



# 02 Adopting Disruptive Tech & AI



## Regulatory Signals

- Model Risk Management
- Complexity & Divergence
- Public Private Partnership

### Signal

Divergent actions at the federal and state levels create risk and compliance challenges:

- Executive directives promote national security and innovation and the removal of regulatory barriers that may hinder it.
- Proliferation of state level laws and regulations, including broad frameworks aimed at developers and/or deployers and narrowly targeted safety and/or privacy laws (e.g., consumer protection, child protection, deepfakes, automated decision-making tools).

### Examples

Federal actions, including:

- Policy recommendations for accelerating AI innovation, infrastructure, and security (e.g., AI Action Plan, EOs for data centers and “full-stack” AI exports)
- Identification of AI technologies constrained due to Federal statutes, regulations, or policies (e.g., OSTP RFI)

State actions (more than 1,000 bills introduced across 50 states in 2025<sup>1</sup>), including:

- “Safety” laws focused on large developers (e.g., CA, NY)
- “Comprehensive” laws for “high risk systems” (e.g., TX)
- Targeted laws (e.g., NY re: child protection)

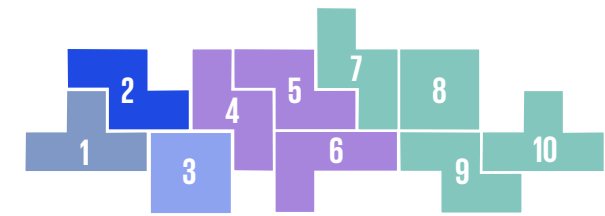
### What to Watch

- Introduction of new laws and regulations, as appropriate, to facilitate recommendations in the AI Action Plan
- Potential revision and/or rescission of federal rules identified as inhibiting AI innovation, infrastructure
- Ongoing introduction of laws and regulations with varying scope and scale across all 50 states; overlaps with cyber, data privacy, and energy infrastructure laws
- Continued calls for federal preemption or moratoriums on enforcement of certain state AI laws
- Potential for increased risks from inaction in the absence or reduction of proactive federal regulatory activity

<sup>1</sup>Derived from Multistate.ai



# 02 Adopting Disruptive Tech & AI



## Regulatory Signals

- Model Risk Management
- Complexity & Divergence
- Public Private Partnership

### Signal

Executive policy to create conditions for private sector-led innovation to flourish and enable AI adoption.

### Examples

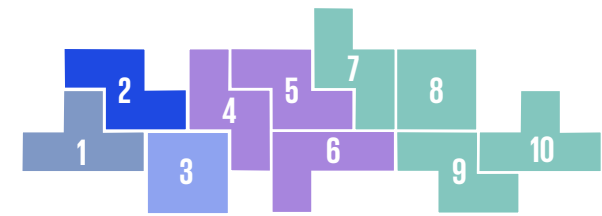
- Promotion (e.g., AI Action Plan) of private sector through access to resources (e.g., models, data), testing facilities (e.g., “regulatory sandboxes”), and industry-specific standards
- Initiatives and projects to facilitate U.S. AI leadership (e.g., EO 14318 re: data centers)
- Private sector-driven innovation for AI applications in payments (e.g., FRB Statement (Waller))

### What to Watch

- Potential changes to regulatory processes, including supervision and rules identified by private industry as inhibiting AI innovation, to better facilitate development and deployment
- Availability of regulatory sandboxes across different agencies
- Streamlined permitting for data center and energy infrastructure along with other incentives at the federal and state levels
- Federal Reserve stakeholder engagement on a "payment account" for fintechs



# 02 Adopting Disruptive Tech & AI



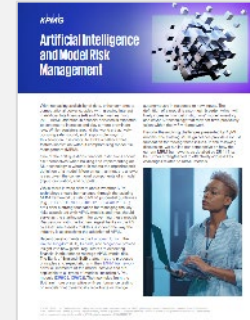
## Regulatory Signals

- Model Risk Management
- Complexity & Divergence
- Public Private Partnership

## Relevant Thought Leadership



[AI Trust: Drive Organizational Value with Confidence](#)



[Artificial Intelligence and Model Risk Management](#)



[2025 Banking Survey: Technology](#)

## Top Related Regulatory Challenges

[03 Maintaining Cyber & Data Security](#)

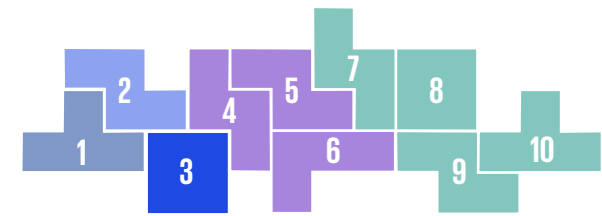
[05 Averting Fraud & Scams](#)

[04 Mitigating Financial Crimes](#)

[06 Protecting Fairness](#)



# 03 Maintaining Cyber & Data Security



## Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- Data Privacy
- Adaptive Frameworks

*Increasingly sophisticated threats to data require organizations and governments to employ advanced technology, adaptive strategies, and skilled professionals to protect critical data and operations.*

*“As we emerge from the era of exploding AI adoption, privacy will be the true differentiating measure of innovation. Leaders’ success won’t be based on how much data they gather, but how wisely and respectfully they steward the information they were entrusted.”*



**Orson Lucas**  
Partner  
Advisory

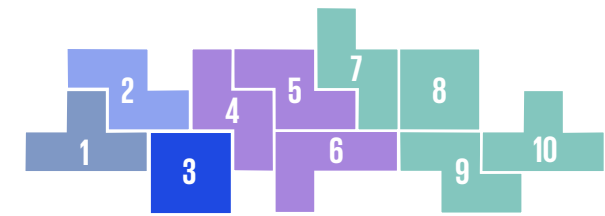
*“Joining the Cyber Risk Institute’s Innovator Program signifies our shared commitment to advancing cyber risk assessment in the financial sector. Through collaboration and supporting industry adoption of the CRI Profile, we aim to enhance the precision and effectiveness of cyber risk assessments, empowering financial institutions to navigate the evolving cyber landscape with confidence.”*



**Matt Miller**  
Principal  
Advisory



# 03 Maintaining Cyber & Data Security



## Regulatory Signals

### Federal Rationalization

• State Complexity & Divergence

• Data Privacy

• Adaptive Frameworks

### Signal

Expressed need for interagency harmonization to align regulatory expectations, reduce overlap, and streamline reporting requirements, including:

- Establishment of single point of cyber coordination.
- Reauthorization of CISA 2015 and funding of CISA to further its role in information/threat sharing.

Information sharing between industry and government is declining due to staffing and funding reductions, and termination of advisory boards.

### Examples

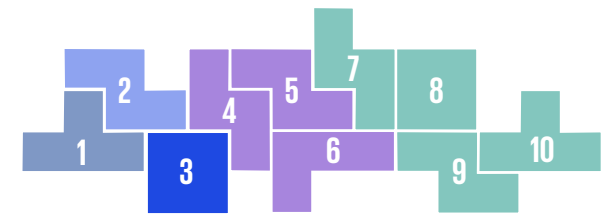
- Alignment of federal cyber efforts (e.g., support for “clean” reauthorization of CISA 2015, ONCD Statement (Cairncross))
- Industry recommendations to “enhance ONCD authority” and “restore CISA capabilities” (e.g., US CSC 2025 Annual Report)
- Formation of industry coalitions to establish standards (e.g., CRI membership and its Financial Services Cyber Security Profile)

### What to Watch

- Release of National Cyber Strategy and “follow-on” action items; anticipated to increase cross-sector agency harmonization
- Potential reauthorization of CISA 2015 and funding for CISA
- Execution of action items in EO 14239, including:
  - Clarification of state role
  - Implementation of a risk-based approach incorporated into the National Resiliency Strategy, National Critical Infrastructure Policy, National Risk Register
- Potential updates to rulemakings (e.g., CISA cyber incident reporting rule, reconsideration of SEC cybersecurity disclosure rule)
- Adoption of the CRI Financial Services Cyber Security Profile and associated Maturity Model



# 03 Maintaining Cyber & Data Security



## Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- Data Privacy
- Adaptive Frameworks

### Signal

Executive directives (e.g., EO 14239, EO 14306) prescribe a more active role in infrastructure resilience and preparedness to the states, resulting in an increase in state legislative activity directed to critical infrastructure and consumers of digital services connected to critical infrastructure.

### Examples

More than 800 cybersecurity bills introduced across 49 states in 2025 with at least 200 bills enacted in 44 states<sup>2</sup>. Focus areas include:

- Agency leadership structures for cyber coordination
- Technical safeguards and best practices
- Compliance and reporting requirements
- Incident response plans

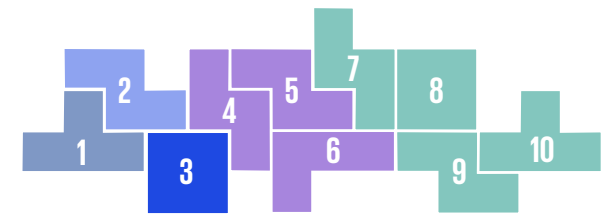
### What to Watch

- Continuing legislative and regulatory activity to strengthen state and local cybersecurity protection related to critical infrastructure and social media; focus areas to include detection, reporting, risk assessment, TPRM, and privacy
- Increasing fragmentation and federal-state and state-state divergence
- Potential skills-based workforce constraints
- Potential rulemaking or policy guidance to clarify federal vs. state cybersecurity roles

<sup>2</sup>Derived from NCSL.org



# 03 Maintaining Cyber & Data Security



## Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- Data Privacy
- Adaptive Frameworks

### Signal

Continued focus at the federal level on national security, sensitive data (e.g., biometric, geolocation), and deepfakes, with a lessened focus on broader consumer protections.

Expansion of state laws and regulations, often in combination with cyber and AI laws, including ongoing attention to children’s privacy and the definition of sensitive data.

### Examples

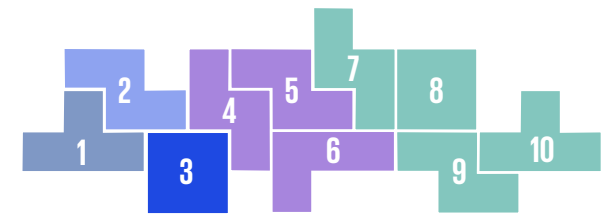
- Restrictions on transfer of sensitive data to select countries (e.g., DOJ bulk sensitive data rule, FCC connected vehicles and subsea cables ownership proposals)
- Development of frameworks to export full-stack AI technology packages (e.g., DOC RFI implementing EO 14320)
- Strengthened protections for children, including “personal data” (e.g., biometric data), data retention and deletion, and parental consent (e.g., FTC COPPA rule, multiple state laws)

### What to Watch

- Forthcoming reconsideration of CFPB Personal Financial Data Rights Rule (Section 1033); potential ongoing legal challenges
- Potential rulemakings related to cross-border data sharing/technology sales
- Increasing compliance challenges, federal-state-global (e.g., India DPDPA, EU-US DPF)
- Strengthened protections for children’s data, sometimes coupled with AI laws and regulations (e.g., verifiable parental consent, unsolicited direct messaging) and expansion of age thresholds (e.g., ages 13-17) with enhanced verification systems
- Ongoing state level enforcement of privacy protections (e.g., CA CCPA actions re: policy disclosure, opt-out rights, data sales)



# 03 Maintaining Cyber & Data Security



## Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- Data Privacy
- **Adaptive Frameworks**

### Signal

Development and application of new approaches to cybersecurity and digital infrastructure, secure software/cloud service providers, and innovative technologies.

### Examples

- Federal contracting requirements to protect sensitive unclassified information, including in supply chains (e.g., DOD CMMC Final Rule)
- Updated standards and security protocols (e.g., NIST Cybersecurity Framework and related guidance)
- Enhanced TPRM expectations to include fourth parties, specific contract requirements, continuous monitoring of vendor security risks, and threat information sharing with critical vendors

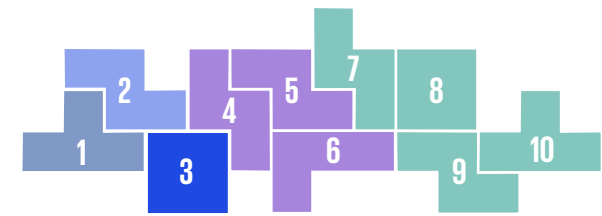
### What to Watch

Expectations for enhanced approaches to cybersecurity and data protection, including:

- Prioritization of data governance, including protections for customer data, models and algorithms, data sharing and protocols for collection, retention, deletion, and archiving
- Governance frameworks designed to be scalable, integrated across the business, informed by lessons learned, and supported by workforce training and development
- Application of new tools (e.g., Security-By-Design principles, AI threat detection systems, quantum-safe encryption)
- Potential increases in regulatory requirements with penalties for noncompliance (e.g., federal, state, global)



# 03 Maintaining Cyber & Data Security



## Regulatory Signals

- Federal Rationalization
- State Complexity & Divergence
- Data Privacy
- Adaptive Frameworks

## Relevant Thought Leadership



[The Importance of an Integrated Approach to Data Privacy Regulations in Cybersecurity](#)



[Cybersecurity considerations 2025: Financial services sector](#)

## Top Related Regulatory Challenges

[02 Adopting Disruptive Tech & AI](#)

[05 Averting Fraud & Scams](#)

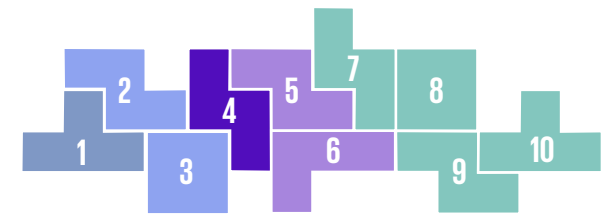
[06 Protecting Fairness](#)

[07 Ensuring Resiliency](#)

[10 Enhancing Parties & Workforce](#)



# 04 Mitigating Financial Crimes



## Regulatory Signals

- “Modernization”
- Recalibration
- Sanctions

*“Modernization” of existing requirements, shaped by the shift to a risk-based approach, new technology applications, dynamic sanctions activity and the Administration’s national security priorities and foreign policy goals.*

*“Practitioners in the AML Compliance space should pay attention to the Administration’s signals around modernization, prioritization of higher risk activities, and regulatory changes. That said, we have not seen any meaningful adjustment in the level of scrutiny afforded the AML program during regulatory exams or other government inquiries, so there is no basis for “taking your foot off the gas” when driving your AML program.”*



**John Caruso**  
Principal  
Advisory

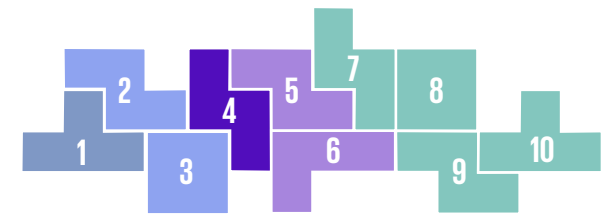
*“As an emerging asset class, predictions markets offer yet another, new avenue for bad actors to launder ill-gotten gains. The growing popularity of the markets is focusing federal and state regulatory attention on necessary guardrails and consumer protections.”*



**DJ Hennes**  
Managing Director  
Advisory



# 04 Mitigating Financial Crimes



## Regulatory Signals

### • “Modernization”

### • Recalibration

### • Sanctions

### Signal

- Ongoing efforts to “reform” supervision and enforcement of the BSA/AML/CFT framework by:
- “Streamlining” BSA/AML/CFT requirements and compliance.
  - Adopting a “risk-based” approach to combatting financial crimes.
  - Shifting focus to “higher risk” activities (e.g., customers, activities) and national security priorities and “deprioritizing lower risk” activities.
  - Considering new technologies or novel approaches to detect illicit activity.

### Examples

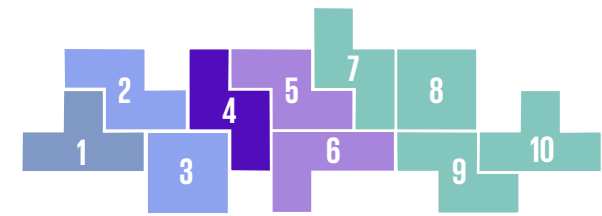
- Clarification of SAR filing requirements and potential for reduced monitoring and documentation regarding “No SAR” dispositions; guidance on evidence of structuring required for SAR filings (e.g., FinCEN FAQs)
- Easing of documentation requirements (e.g., FinCEN Exemptive Order for the CIP Rule permitting alternate sources)
- Discussing the “need to modernize,” including through innovation and allocation of limited resources (e.g., Treasury Statements (Bessent, Hurley), FinCEN Testimony (Gacki))
- Solicitation for comment on innovative approaches (e.g., Treasury RFI)
- Extended effective date of RIA AML Program rule, with extended comment period

### What to Watch

- Potential rulemakings, including:
  - Final rule requiring financial institutions to incorporate the AML/CFT priorities into a risk-based AML/CFT program (as included in published regulatory agendas)
  - Proposal to implement BSA provisions of the GENIUS Act
  - Proposal to establish a whistleblower awards program for violations of BSA and sanctions laws
- Potential changes to the AML/CFT framework to focus on national security and highest risk areas and explicitly permit financial institutions to de-prioritize lower risks
- Potential for increased risk in “lower risk” (i.e., lower priority) areas; fintech partnership may pose heightened BSA/AML risk



# 04 Mitigating Financial Crimes



## Regulatory Signals

- “Modernization”
- **Recalibration**
- Sanctions

### Signal

Prioritization of “higher risk” activities in addition to the Administration’s national security priorities (e.g., terrorist financing, cybercrime, fraud, sanctions evasion, and human and drug trafficking), with heightened attention to activities of cartels and TCOs and entities that materially support them. At the same time, narrowing the application of certain regulations to recalibrate the regulatory focus.

### Examples

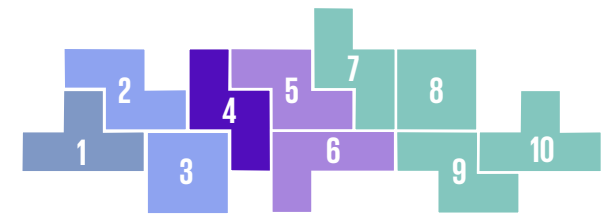
- Executive directives aimed at cartels and TCOs (e.g., EO 14157, EO 14161)
- Prioritization of FCPA investigations and enforcement to focus on cartels and TCOs (e.g., DOJ Memo)
- Setting limitations on required reporting entities (e.g., FinCEN rule re: CTA BOI reporting to foreign entities)
- Outlining considerations for innovative or novel approaches to detect illicit activity involving digital assets (e.g., PWG Report)

### What to Watch

- Potential legislative and/or regulatory “reforms” to adopt innovative processes such as AI, blockchain analytics, digital identity, and APIs as part of the AML framework
- Rule proposal to implement BSA provisions of the GENIUS Act, including “tailoring” for the stablecoin industry
- Continuing Congressional efforts to increase the SAR and CTR dollar thresholds



# 04 Mitigating Financial Crimes



## Regulatory Signals

- “Modernization”
- Recalibration
- **Sanctions**

### Signal

Increasing use of sanctions and secondary sanctions to achieve national security and foreign policy goals, including against non-traditional targets (e.g., International Criminal Court).

### Examples

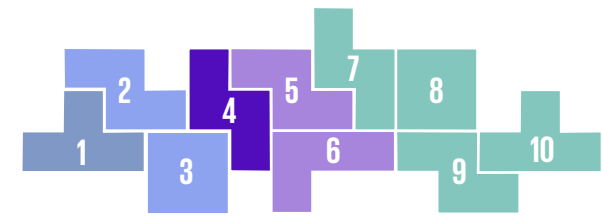
- Imposition of sanctions aligned to foreign policy goals (e.g., targeting international drug trafficking)
- OFAC designation of multiple TCOs as terrorist groups (e.g., EO 14157)

### What to Watch

- Ongoing and prominent use of sanctions (e.g., imposition, expansion, rescission) to reinforce national security and foreign policy goals, including global economic trade
- Continuation of existing sanctions programs (e.g., SDN list, secondary sanctions, sectoral sanctions)
- More responsibility to identify illicit activity/sanctions evasion to shift to financial institutions as regulators focus on stated priorities (e.g., DOJ)



# 04 Mitigating Financial Crimes



## Regulatory Signals

- “Modernization”
- Recalibration
- Sanctions

## Relevant Thought Leadership



[Financial Crime: Regulatory Shifts, Supervisory Focus, and Emerging Risk](#)



[Rapidly changing regulatory landscape](#)



[Risk management redefined](#)



[Sports Betting Risks: AML and Fraud in Focus](#)

## Top Related Regulatory Challenges

[02 Adopting Disruptive Tech & AI](#)

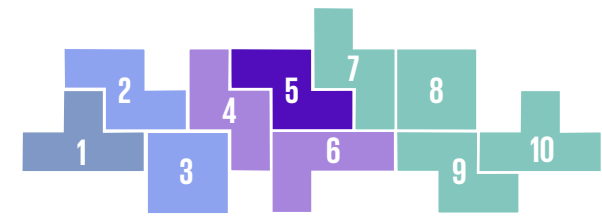
[03 Maintaining Cyber & Data Security](#)

[05 Averting Fraud & Scams](#)

[09 Expanding Digital Assets](#)



# 05 Averting Fraud and Scams



## Regulatory Signals

- “Fast & Furious”
- Reprioritizing Enforcement
- Trends

*Traditional frauds and scams are giving way to a new generation of rapidly evolving AI-enhanced activities carried out at scale, significantly raising the importance of effective risk management and reporting.*

*“The speed and sophistication with which fraudsters are now able to exploit AI and emerging technologies is outpacing traditional defenses. To effectively mitigate these threats, regulators, companies, governments, and law enforcement must break down silos and collaborate more openly—sharing the data they sit on and coordinating responses in real time. Fragmented efforts are no longer sufficient in a world where fraud evolves faster than policy.”*



**Steve D’Antuono**  
Partner  
Advisory

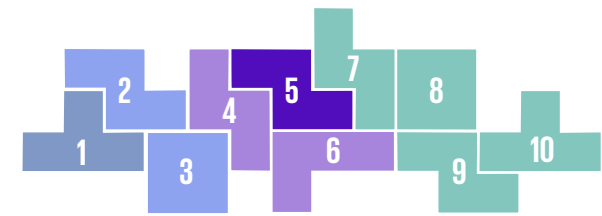
*“Emerging market dynamics, including open banking, digital assets, and M&A activity, are reshaping financial services and creating novel fraud risks. Financial institutions must guard against fragmentation and ensure cross-functional coordination to stay ahead of fraudsters and protect consumers.”*



**Chad Polen**  
Principal  
Advisory



# 05 Averting Fraud and Scams



## Regulatory Signals

- “Fast & Furious”
- Reprioritizing Enforcement
- Trends

### Signal

Attributable largely to technology innovation (and primarily AI and GenAI), the speed, scale, and complexity of frauds and scams have significantly increased, rising to historic levels of volume and cost. These tools “turbocharge” sophisticated frauds and scams (e.g., impersonation, instant payment, deepfakes and social engineering), driving the need for a cohesive regulatory approach across functions within the organizations to detect, prevent, and mitigate these crimes.

### Examples

- \$12.5B in reported losses, a 25% year-over-year increase; 800M+ imposter scams reported<sup>3</sup>
- “Cyber-enabled fraud” (using internet or other technology) accounted for more than 80% of all reported losses<sup>4</sup>
- Recommendation for a “government-wide” strategy to counter scams and improve complaints reporting, consumer education, and federal coordination (e.g., GAO Report)

### What to Watch

- Heightened regulatory attention to the effectiveness of fraud risk management programs, including TPRM, data sharing, and complaints analysis, to monitor, detect, and mitigate threat actors as well as keep pace with evolving threats
- Potential for more categories of fraud and scams to be reported
- Potential for escalation in the scale and sophistication of frauds and scams to be elevated to a national security issue leading to executive, legislative, and/or regulatory action
- Forthcoming NACHA fraud monitoring rules for ACH payments

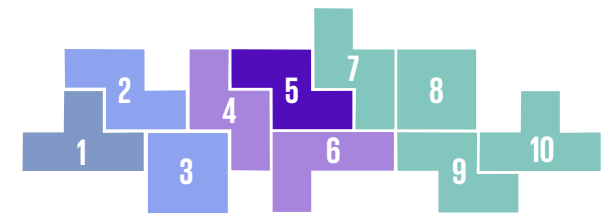
<sup>3</sup>2024 FTC Data Book (most recently available information as of 11/2025)

<sup>4</sup>FBI 2024 IC3 (most recently available information as of 11/2025)





# 05 Averting Fraud and Scams



## Regulatory Signals

- “Fast & Furious”
- Reprioritizing Enforcement
- Trends

### Signal

To carry out executive directives, federal agencies are prioritizing fraud investigation and enforcement related to healthcare; procurement; trade, tariffs, and customs evasion; sanctions evasion and support for cartels and TCOs; securities and other market manipulations; and vulnerable persons (e.g., elders, servicemembers).

### Examples

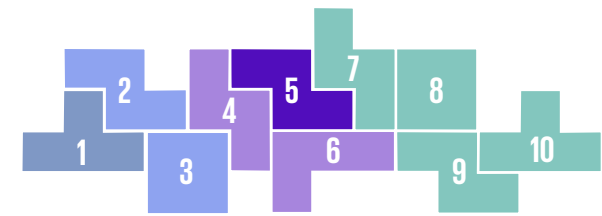
- Enforcement policy changes addressing “unchecked fraud in U.S markets and government programs” (e.g., DOJ Memo on White Collar Crime)
- Redirected supervision to actual fraud against identifiable victims with material and measurable damage (e.g., CFPB Staff Memo)
- Facilitating the ability to identify overpayments and fraud in government activities (EO 14243) along with FCA enforcement
- Interagency collaboration (e.g., DOJ/DHS Trade Fraud Task Force)
- Heightened enforcement (e.g., DOJ actions under FCA, SEC Cyber and Emerging Technologies Unit)

### What to Watch

- Broad application of the FCA to include new (nontraditional) areas, such as trade, employment verification, and civil rights
- Continued FCA enforcement in priority areas (e.g., healthcare; government contracts; trade, tariff, and customs)
- Focus on retail investor protections, including misuse of technology to commit fraud and false or misleading statements about the use of technology (e.g., SEC)



# 05 Averting Fraud and Scams



## Regulatory Signals

- “Fast & Furious”
- Reprioritizing Enforcement
- Trends

### Signal

Financial institutions, organizations, and consumers are facing a myriad of frauds and scams, exacerbated by digital assets, open banking and M&A activities. Key among them are:

- Impersonation scams, including business email compromise scams
- Deepfake/AI enabled scams
- “Faster” payments and “instant” payments scams (and relatedly increased attention to liability/consumer reimbursement)
- Synthetic identity fraud, identity theft and account takeovers
- Check fraud
- Elder abuse/vulnerability exploitation

### Examples

- Data aggregation/reporting of fraud- and scam-related complaints (e.g., Annual FTC Data Book; Annual FBI IC3)
- Regulatory alerts highlighting areas of rising risk (e.g., FinCEN Alerts re: virtual currency kiosks)
- Public service campaigns and consumer-oriented materials on detecting and mitigating frauds and scams (e.g., multiple posts by FBI, FRB, FTC)
- Solicitation for public comments on ways to mitigate fraud (e.g., interagency RFI on payments fraud)
- Introduction of laws and regulations to enhance consumer protections (e.g., 1000+ state bills in 2025 related to AI<sup>5</sup>, privacy, or cybersecurity)

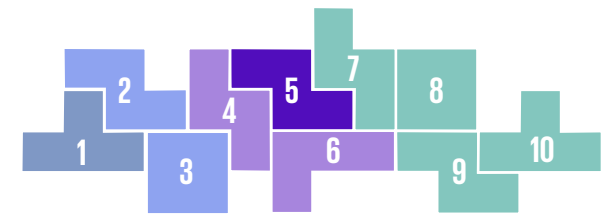
### What to Watch

- The sophistication and variety of frauds and scams will evolve more quickly than regulatory frameworks - bad actors are more flexible than regulators
- Potential for new frauds and scams to be developed around digital assets (e.g., false products, exchanges, websites, apps) as they gain broader market presence

<sup>5</sup>Derived from Multistate.ai



# 05 Averting Fraud and Scams



## Regulatory Signals

- “Fast & Furious”
- Reprioritizing Enforcement
- Trends

## Relevant Thought Leadership



[Modernize your dispute and fraud case management](#)



[KPMG Global Banking Scam Survey](#)

## Top Related Regulatory Challenges

[02 Adopting Disruptive Tech & AI](#)

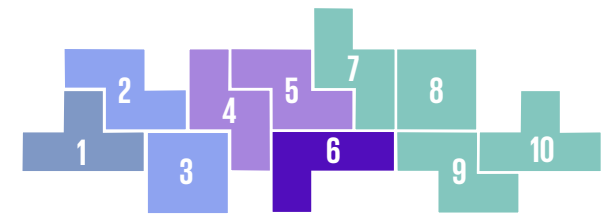
[04 Mitigating Financial Crimes](#)

[03 Maintaining Cyber & Data Security](#)

[06 Protecting Fairness](#)



# 06 Protecting Fairness



## Regulatory Signals

- Fair Access
- Fairness in Focus
- AI Influence
- Direct Harm

*Though in part redefined by executive actions, “fairness” laws continue in force with ongoing attention to disclosure clarity and accuracy, “access” to banking, and the use of AI.*

*“Risk and Business leaders are recommended to revisit the core principles of their fairness programs with a particular focus on equal access and uses of AI.”*



**Mike Lamberth**  
*Partner  
Advisory*

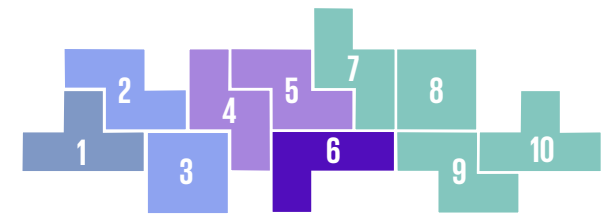
*“As regulators ease historical constraints on the types of products accessible to main street investors, companies will need to be diligent in the execution of their suitability and fiduciary responsibilities.”*



**Mike Sullivan**  
*Principal  
Advisory*



# 06 Protecting Fairness



## Regulatory Signals

- Fair Access
- Fairness in Focus
- AI Influence
- Direct Harm

### Signal

Executive directives have set expectations for assuring fair access to products, services, and opportunities for consumers and organizations alike (e.g., banking services, internet access, health care, prescription drugs).

### Examples

Practices perceived to result in denying services to some individuals/entities are targeted by executive directives, including those based on:

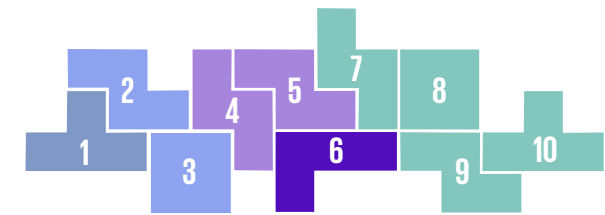
- Political or religious beliefs, affiliations, or business (e.g., EO 14331)
- Failure to meet certain investment criteria (e.g., EO 14330)
- Presumption rather than a policy, practice, or intent (e.g., EO 14281)
- Unfair/noncompetitive practices within a specific industry (e.g., EO 14254 , EO 14297)

### What to Watch

- In financial services, heightened attention to potential issues related to “debanking,” “disparate impact,” and “suitability”
- Potential for prolonged uncertainty as to whether a new standard of “fairness” will take shape or the role that states may play to help set and enforce it



# 06 Protecting Fairness



## Regulatory Signals

- Fair Access
- **Fairness in Focus**
- AI Influence
- Direct Harm

### Signal

Fairness continues to be the law. Long standing consumer and investor protection laws (e.g., ECOA, FHA, FTC Act) and their implementing regulations remain intact and assessed in supervisory examinations. Federal regulators continue to emphasize their expectations for organizations to embed fairness into services and practices, alongside increasing state legislative and enforcement activity.

### Examples

Targeted actions to protect fair access/fair treatment include:

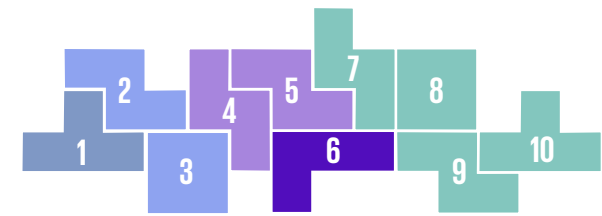
- Building fairness into goals and strategies (e.g., FTC Strategic Plan)
- Providing transparency on processes and expectations (e.g., DOJ Memo on White Collar Crime)
- Eliminating “reputation risk” from supervisory materials (e.g., bank interagency proposal); prohibiting denial of services based on non-risk-based criteria (e.g., state laws introduced in AZ, GA, ID)
- Requiring clear and truthful representations/disclosure (e.g., FTC Final Rule on Unfair or Deceptive Fees )
- Restricting the use of automated decision-making tools/systems for lending practices (e.g., state laws introduced in RI, NY)
- Considering retail investor access to private funds (e.g., SEC Statements (Atkins, Uyeda))

### What to Watch

- Expectations for clear, true, and complete representations/disclosure in consumer/investor-facing materials
- Recommendations provided to retail investors align with the customer’s risk profile, are fair and unbiased, and in the best interest of the customer
- Heightened scrutiny of adverse decisions in providing services



# 06 Protecting Fairness



## Regulatory Signals

- Fair Access
- Fairness in Focus
- **AI Influence**
- Direct Harm

### Signal

Heightened awareness of the potential for bias in AI applications (e.g., lending, employment, healthcare decisions). High degree of state-level legislation/regulation to apply “unfair or deceptive acts or practices” standards to AI systems.

### Examples

Actions to mitigate the potential for bias including:

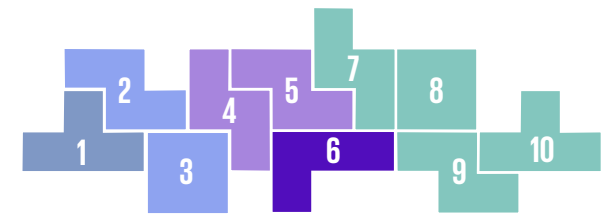
- Applying antitrust laws to ensure market incumbents do not hinder newcomers or startups (e.g., DOJ Speech (Slater) on real competition in AI)
- Considering applications substantially developed by AI to not be original ideas “to maintain fairness and originality” (e.g., NIH 2025 Policy)
- Applying anti-bias/fair lending laws to lending and pricing decisions made by AI or automated technology tools (e.g., CA, MA, NJ State AGs); prohibiting pricing algorithms trained on competitor data (e.g., CA, OH state bills)
- Adopting “comprehensive” AI bills (e.g., state laws (CO, UT))

### What to Watch

- Potential for legislation/regulation at the federal or state level to incorporate requirements for transparency, accountability, and bias mitigation



# 06 Protecting Fairness



## Regulatory Signals

- Fair Access
- Fairness in Focus
- AI Influence
- **Direct Harm**

### Signal

Shifting supervision and enforcement to focus on instances where there is clear intent to “victimize” consumers/investors and “tangible harm” or “actual fraud.”

### Examples

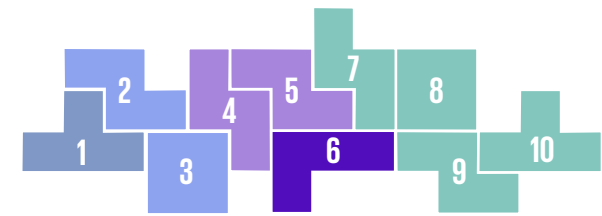
- Focusing investigations on “tangible harm to consumers,” returning funds to victims rather than penalizing organizations (e.g., CFPB Staff Memo)
- Dropping investigations/lawsuits against organizations that do not have clear criminal intent or obvious victims (e.g., DOJ)

### What to Watch

- State AGs are expected to intensify activity across a wider range of financial products and services and across an array of providers
- Expect increased collaboration through multi-state investigations



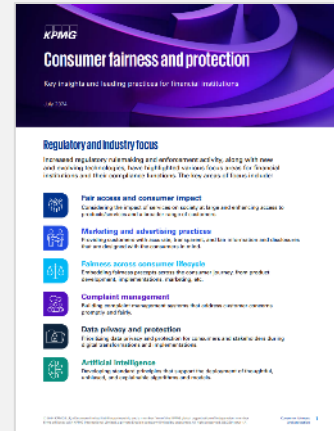
# 06 Protecting Fairness



## Regulatory Signals

- Fair Access
- Fairness in Focus
- AI Influence
- Direct Harm

## Relevant Thought Leadership



[Consumer Fairness and Protection: Key Insights and Leading Practices for Financial Institutions](#)

## Top Related Regulatory Challenges

[02 Adopting Disruptive Tech & AI](#)

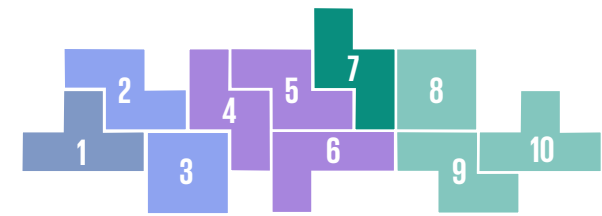
[05 Averting Fraud & Scams](#)

[08 Driving Capital Formation & Growth](#)

[09 Expanding Digital Assets](#)



# 07 Ensuring Resiliency



## Regulatory Signals

- Business Continuity & Resiliency Planning
- Technology Interconnectedness
- Capital & Liquidity

*A growing focus on organizations’ preparedness to withstand or recover from significant market stresses and disruptions that may impact non-financial operations (e.g., cybersecurity, technology) and financial risks (e.g., capital, liquidity).*

*“As banks advance their ambitions for expanded reach, management teams must operationalize strategic roadmaps that will enable them to thrive with a more competitive peer group.”*



**KB Babar**  
Principal  
Advisory

*“Resilience is not achieved through isolated disciplines. Operational Resilience, Business and IT Continuity, and Incident and Crisis Management must converge into a single, integrated program—one that anticipates, absorbs, and adapts to disruption. Only through harmonized processes and unified oversight can organizations build the agility and strength required to thrive in an increasingly uncertain world.”*



**Prince Harfouche**  
Principal  
Advisory

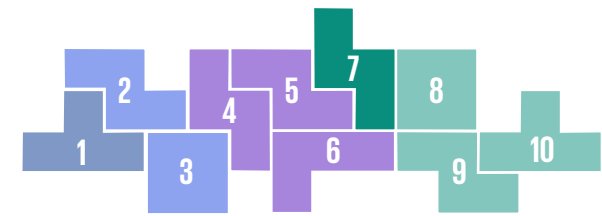
*“Tools such as AI and cloud services add complexities to an already complicated and interconnected environment. The speed with which these technologies are changing and the increasing reliance on them means organizations must continuously adapt their risk management, compliance, and operational strategies to keep pace with evolving threats and opportunities.”*



**David Tarabocchia**  
Principal  
Advisory



# 07 Ensuring Resiliency



## Regulatory Signals

- **Business Continuity & Resiliency Planning**
- Technology Interconnectedness
- Capital & Liquidity

### Signal

In response to increasing threats to information and technology security and complex interdependencies (e.g., supply chains, third-party service providers), regulators expect organizations to develop plans addressing critical functions, service-level agreements, and significant disruptions. Areas of focus include:

- Plan creditability (to maintain business continuity).
- Testing for critical operations and related third parties.

Consideration of easing expectations for some entities given certain overlapping requirements.

### Examples

Actions from financial services regulators, including:

- Planning focused on “most relevant” information (e.g., FDIC FAQ)
- Potential easing of overlapping requirements (e.g., FDIC Statement (Hill) re: filers of FDIC IDI Rule and FDIC/FRB Title I plans; CFTC withdrawal of proposed operational resilience framework)
- Scrutiny of catastrophe resilience, pre-disaster planning, and cybersecurity (e.g., state laws related to P&C insurance)

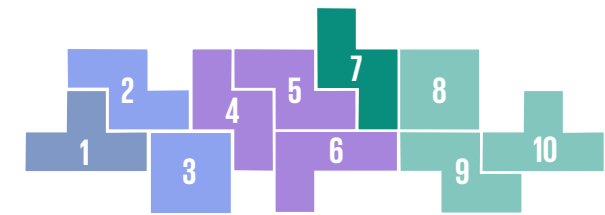
Actions from other regulators including requirements for medical device supply chain disruption reporting (FDA) and data sharing on grid reliability (DOE).

### What to Watch

- Possible FDIC proposal to, at a minimum, codify its 2025 FAQs into the agency’s IDI Rule and potentially also to streamline elements of the IDI Rule; concurrent consideration of streamlining requirements for entities filing pursuant to both the IDI Rule and the Title I Rule for BHCs
- Forthcoming compliance requirements with the OCC Recovery Planning Guidelines (staggered requirements beginning January 1, 2026) alongside a proposal to withdraw the Guidelines and related planning requirement
- Evolving/expanding regulatory expectations around operational resilience risk management practices (e.g., identifying critical operations and mapping interdependencies)
- Continued interagency collaboration on operational resilience



# 07 Ensuring Resiliency



## Regulatory Signals

- Business Continuity & Resiliency Planning
- Technology Interconnectedness
- Capital & Liquidity

### Signal

Elevated levels of operational risk reinforce the importance of operational and technology resilience, business continuity and incident response plans.

Risk attributed to cybersecurity and technology management largely due to third-party concentrations (e.g., cloud providers, FMUs, “off the shelf” software), increasingly sophisticated threat actors, and prolonged use of legacy systems.

### Examples

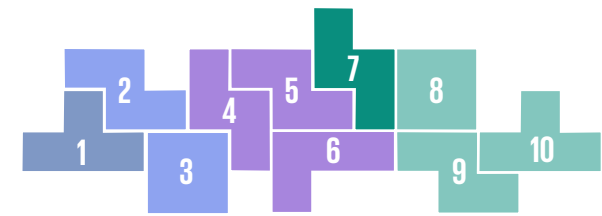
- OCC Semi-Annual Risk Perspective 2025
- OCC, FDIC 2025 Reports on Cybersecurity and Resilience
- Near-term risks in cyber resiliency and TPRM (e.g., FRB Statement (Barr))
- Top key risks including concentration risk, emerging technologies, and tech vulnerabilities (e.g., Treasury Financial Sector Risk Management Plan)

### What to Watch

- Continued interagency coordination on operational resilience and cybersecurity supervision for large, complex, interconnected entities and significant third parties engaged in the delivery of critical services
- Continued interagency participation in FFIEC committees on cybersecurity, critical infrastructure and IT to share and align supervisory practices and efforts
- Potential reforms to IT examinations
- Heightened regulatory expectations for concentration risk assessments and contingency planning for critical service provider outages
- Potential for changing expectations related to cyber and ICT risk management, incident reporting, and third-party risk management along with resiliency planning, monitoring, and testing based on international requirements (e.g., DORA)



# 07 Ensuring Resiliency



## Regulatory Signals

- Business Continuity & Resiliency Planning
- Technology Interconnectedness
- Capital & Liquidity

### Signal

Actions to tailor regulatory requirements for elements of capital and liquidity based on institution size and risk, as well as providing for increased attention to transparency and accountability.

### Examples

- Consideration of capital “modernizations” including stress testing, Basel III, community bank tailoring, indexing thresholds (e.g., Statements from FRB, FDIC, Treasury (Bowman, Hill, Bessent))
- Proposal to amend the ESLR (e.g., FRB, OCC, FDIC Interagency release)
- Proposals to reduce stress testing volatility and increase transparency (e.g., FRB, OCC, FDIC interagency release)
- Delay and reevaluation of liquidity risk management reporting (e.g., SEC Form N-PORT)

### What to Watch

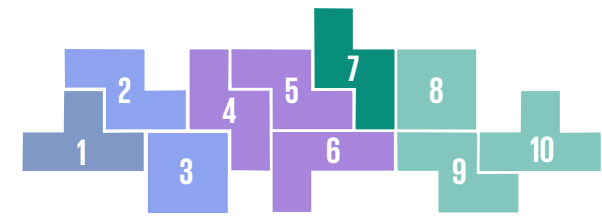
Continued focus on capital and liquidity “modernization” including:

- Final interagency rules on ESLR, transparency in stress test models and scenario development, and averaging of stress test results and related stress capital buffer
- Revision of the Basel III Endgame proposal
- Tailoring of community bank capital requirements, including the CBLR

Reassessment of the liquidity framework including:

- The role of the discount window and FHLBs
- Access to Federal Reserve “master accounts” as well as consideration of “skinny master accounts”
- Potential OCC codification of contingency funding plan expectations

# 07 Ensuring Resiliency



## Regulatory Signals

- Business Continuity & Resiliency Planning
- Technology Interconnectedness
- Capital & Liquidity

## Relevant Thought Leadership



[Be organizationally and operationally resilient when—and where—it matters](#)



[Operational Resilience](#)

## Top Related Regulatory Challenges

[01 Executing Mandates](#)

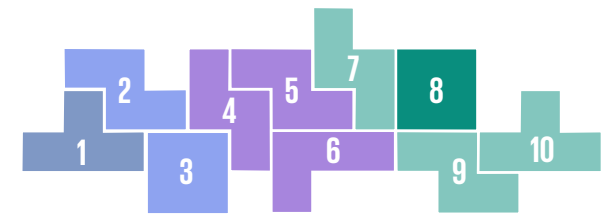
[03 Maintaining Cyber & Data Security](#)

[08 Driving Capital Formation & Growth](#)

[10 Enhancing Parties & Workforce](#)



# 08 Driving Capital Formation & Growth



## Regulatory Signals

- Private Credit
- IPO Revitalization
- Retail Access & Protections
- Bank Formation
- Mergers & Acquisitions

*Focus on capital-raising sources to promote economic growth and innovation, including private credit, public markets, and the role of retail investors.*

*“The likely continuation of decreasing interest rates will drive M&A and IPO activity. For banks, size and scale will matter as they face the challenges of AI adoption and a rapidly changing regulatory environment; developing a strategy will be challenging given market sentiment that remains unpredictable.”*



**Henry Lacey**  
Principal  
Advisory

*“Accelerated regulatory approvals are driving an uptick in large-scale banking M&A and regional bank consolidation, with the approval window for major deals now shortened to approximately three months.”*



**Nadia Orawski**  
Principal  
Advisory

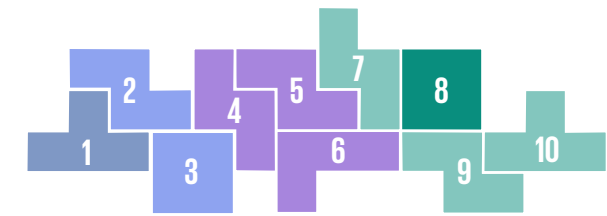
*“This is a time of both opportunities and risks. Easing of regulatory constraints and the rise of private assets means companies will need to evolve their risk and compliance programs to protect their customers and their own reputations.”*



**Mike Sullivan**  
Partner  
Advisory



# 08 Driving Capital Formation & Growth



## Regulatory Signals

- **Private Credit**
- IPO Revitalization
- Retail Access & Protections
- Bank Formation
- Mergers & Acquisitions

### Signal

Rapidly expanding segment of nonbank financial intermediaries highlights a shift from traditional bank financing to alternative sources. Regulatory concerns include the potential for elevated systemic risk through interconnectedness with other financial entities, combined with a lack of transparency or reporting on private credit market participants.

### Examples

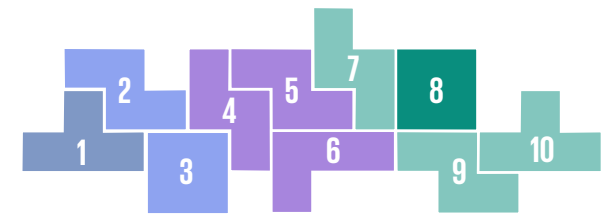
- Research investigating interdependencies among banks, BDCs, and PD funds, focusing on systemic vulnerabilities and financial stability (e.g., FedNotes, May 2025: Bank Lending to Private Credit)
- Identification of NDFI lending and private credit as a key credit risk (e.g., FDIC 2025 Risk Review)
- Identification of potential financial stability risks related to NDFIs and private credit (e.g., most recent FSOC Annual Report)

### What to Watch

- Potential reconsideration of proposals for new data collection and reporting requirements on NDFI lending (e.g., Call Report)
- Potential for increased supervisory focus and oversight of non-bank lending practices, such as:
  - Capital, liquidity stress testing, resiliency, private fund securitization disclosures (e.g., Form PF)
  - Credit/funding chains (e.g., bank lending, BDCs, and borrowers)
  - Enhanced loss analysis and impact on CECL reserves
  - Market conduct (e.g., conflicts of interest)
  - Investor protections, NDFI governance and risk management



# 08 Driving Capital Formation & Growth



## Regulatory Signals

- Private Credit
- IPO Revitalization
- Retail Access & Protections
- Bank Formation
- Mergers & Acquisitions

### Signal

Responding to an extended decline in the number of IPOs, regulators (and legislators) seek to revitalize the attractiveness of IPOs as a means of raising capital (e.g., easing requirements such as reduced documentation and investor communications as well as scaling certain requirements post-IPO) and bringing more investment opportunity and diversification to the public markets.

### Examples

Recent activity from the SEC includes:

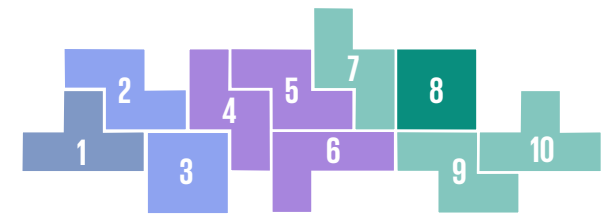
- Commissioner Statements (Atkins, Uyeda)
- Enhanced accommodations for issuers submitting draft registration statements for nonpublic review
- Policy revisions to permit mandatory arbitration in registration statements

### What to Watch

- Potential SEC rulemaking for emerging growth companies to include:
  - Definitions and qualifications
  - New accommodations for existing disclosure requirements
  - Enhanced accommodations and simplification of filer status for reporting companies
- Shareholder proposal “modernization”



# 08 Driving Capital Formation & Growth



## Regulatory Signals

- Private Credit
- IPO Revitalization
- **Retail Access & Protections**
- Bank Formation
- Mergers & Acquisitions

### Signal

Intended expansion of retail investor access, with safeguards, to invest in private market opportunities, giving consideration to ideas such as:

- Amending rules for accredited investors and exempt offerings.
- Permitting retail investment (through funds) to invest in private funds.

### Examples

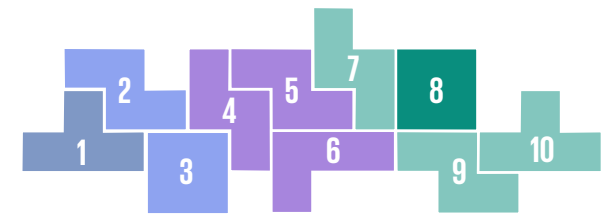
- Allowing retail investor access to alternative assets in ERISA plans (e.g., EO 14330)
- Consideration of changes to accredited investor qualifications, exempt offering requirements (e.g., SEC Statements (Uyeda))
- Removing investment limitations on closed-end funds (e.g., SEC Division of Investment Management, ADI 2025-16)

### What to Watch

- Rulemaking from the DOL and other regulators to facilitate retail access to private markets through ERISA plans and related fiduciary responsibilities
- Regulatory (e.g., SEC) and legislative efforts to amend accredited investor qualifications, including non-financial criteria
- Potential updates to existing rules/frameworks to strengthen investor protections where retail investors may access private markets, and to facilitate capital formation
- More product offerings that give indirect exposure to private funds



# 08 Driving Capital Formation & Growth



## Regulatory Signals

- Private Credit
- IPO Revitalization
- Retail Access & Protections
- **Bank Formation**
- Mergers & Acquisitions

### Signal

Acceptance of new bank entrants/models to accommodate changes in the financial markets; areas considered include:

- ILCs, de novo bank charters.
- Revisions to expand eligibility of private equity and other nonbank entities to bid for failed banks.

### Examples

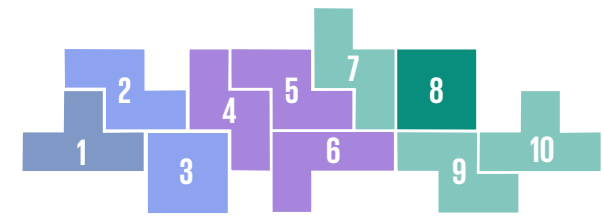
- OCC preliminary approval of de novo bank charter focused on digital assets; reinstatement of “streamlined application and expedited review procedures”
- Consideration of private equity bidders (e.g., FDIC Statement (Hill))
- Review of “nature and structure” of non-financial companies forming an industrial bank (e.g., FDIC RFI on ILCs)

### What to Watch

- Launch of FDIC pilot program for a nonbank bidder pre-qualification process (January 2026)
- OCC approvals of de novo bank charter applications as well as national trust bank charters related to stablecoin custody
- Potential reconsideration of FDIC ILC framework



# 08 Driving Capital Formation & Growth



## Regulatory Signals

- Private Credit
- IPO Revitalization
- Retail Access & Protections
- Bank Formation
- **Mergers & Acquisitions**

### Signal

Continued application of existing guidance focusing on anti-competitive transactions to maintain open, competitive markets and encourage innovation.

Executive directives will impact cross-border transactions in areas related to global supply chains, tariffs, “critical technologies,” and national security.

### Examples

- Identification of anti-competitive regulations for potential reconsideration (e.g., DOJ, FTC RFI)
- Withdrawal of appeal to non-compete rule challenge (e.g., FTC)
- Solicitation on the scope, prevalence, and effect of employer non-compete agreements (e.g., FTC RFI)

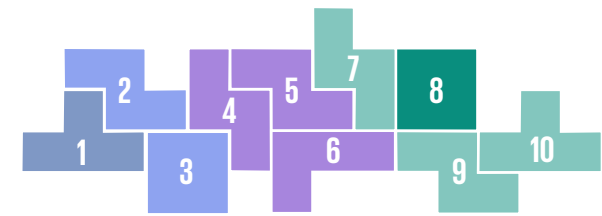
### What to Watch

2026 deal-making may be driven by multiple factors including:

- Acquisition of technology and related talent
- Economic conditions (e.g., falling interest rates)
- The regulatory environment (e.g., banking agency statements re: timely reviews; changes to HSR reviews)
- Capital reallocation (e.g., based on tariffs/supply chains)



# 08 Driving Capital Formation & Growth



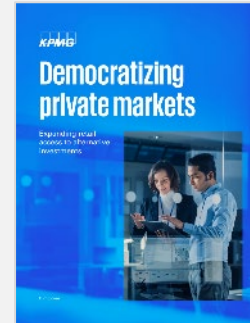
## Regulatory Signals

- Private Credit
- IPO Revitalization
- Retail Access & Protections
- Bank Formation
- Mergers & Acquisitions

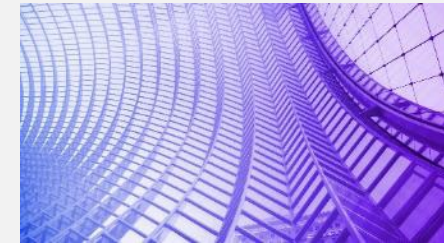
## Relevant Thought Leadership



[How regional and community banks can thrive in a fast-changing market](#)



[Democratizing private markets](#)



[Capital markets and investment management](#)

## Top Related Regulatory Challenges

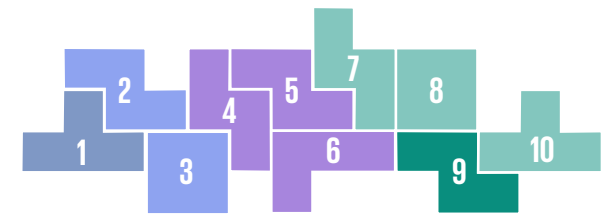
[06 Protecting Fairness](#)

[07 Ensuring Resiliency](#)

[09 Expanding Digital Assets](#)



# 09 Expanding Digital Assets



## Regulatory Signals

- Frameworks
- Risk Considerations
- Licensing/Chartering
- Access

**Accelerating and widespread actions designed to structure markets and develop regulatory frameworks that will facilitate and expand digital and other alternative asset offerings in the U.S.**

*“Digital assets have once again taken center stage, spotlighted by the rescission of regulatory guidance and the passage of the GENIUS Act which will give rise to payment stablecoins. Banks must develop digital asset strategies for a new asset class and technology that have not historically been part of their business model, along with identifying what products/services to offer and related risk considerations and mitigation controls.”*



**Brian Consolvo**  
Principal  
Advisory

*“The regulatory environment has shifted radically in 2025, and many financial institutions are moving quickly to offer digital asset products and services. Given the rapid pace of change, it’s more important than ever for organizations to assess and enhance their compliance and risk management programs.”*



**Conway Dodge**  
Principal  
Advisory

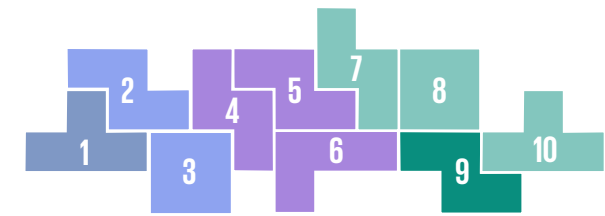
*“As barriers to broader adoption of digital assets abate, and competition and demand significantly increase, banks will need to quickly evolve business models, product/ service offerings, and risk management practices to take and grow market share in a safe and sound, consumer-centric manner.”*



**Todd Semanco**  
Partner  
Advisory



# 09 Expanding Digital Assets



## Regulatory Signals

- Frameworks
- Risk Considerations
- Licensing/Chartering
- Access

### Signal

Executive and legislative steps to establish/build-out frameworks governing digital assets.  
 Concurrent agency initiatives to update existing rules/requirements to promote digital assets markets.

### Examples

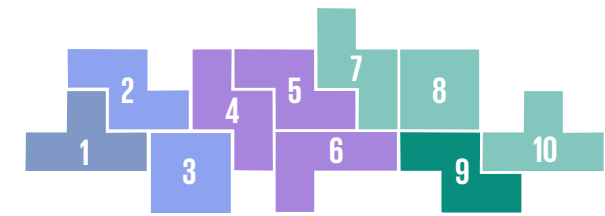
- Legislation defining a framework for digital assets (e.g., payment stablecoins framework established by P.L. 119-27, GENIUS Act)
- Market structure legislation setting regulatory responsibilities for cryptocurrencies (e.g., CLARITY Act as passed by the House)
- Roadmap for building out tokenized assets (e.g., PWG Report)
- Directives to strengthen blockchain technology (e.g., EO 14178)
- Agency initiatives (e.g., SEC Project Crypto, CFTC Crypto Sprint)

### What to Watch

- Implementation of the GENIUS Act, including forthcoming final regulations due July 2026 (i.e., FDIC, FRB, NCUA, OCC, state regulators)
- Potential passage of “market structure” legislation (e.g., CLARITY Act) setting SEC/CFTC jurisdictions and asset classifications
- New and amended SEC/CFTC rulemakings to carryout PWG Report recommendations, including re: digital securities and commodities definitions, licensing/ registration requirements, custody, on-chain systems, and exemptions/safe harbors



# 09 Expanding Digital Assets



## Regulatory Signals

- Frameworks
- Risk Considerations
- Licensing/Chartering
- Access

### Signal

Identification of a full spectrum of risks to manage new digital asset products/frameworks, including market, capital/liquidity, operational (e.g., cybersecurity, technology), fraud/BSA/AML, and consumer/investor protections, including education/disclosures.

### Examples

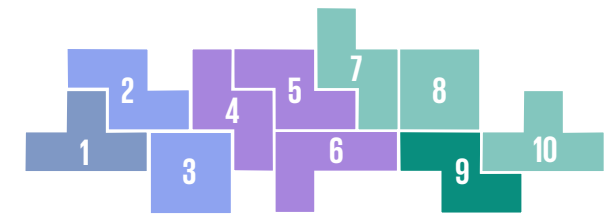
- SEC Crypto Task Force and public outreach through public meetings/roundtables
- Statutorily required risk management and compliance requirements (e.g., P.L. 119-27, the GENIUS Act)
- Market structure legislation for cryptocurrencies setting regulatory responsibilities (e.g., CLARITY Act as passed by the House)
- Federal banking agency guidance (e.g., focus on risk management, safety and soundness)

### What to Watch

- Regulatory scrutiny consistent with existing risk and compliance framework (e.g., capital/liquidity, BSA/AML, consumer/investor protections, TPRM)
- Integration of digital asset offerings with traditional banking services (e.g., custody, trading, credit card rewards)
- Use of interpretive, exemptive, and other authorities (e.g., sandboxes) to promote innovation in novel areas



# 09 Expanding Digital Assets



## Regulatory Signals

- Frameworks
- Risk Considerations
- Licensing/Chartering
- Access

### Signal

Expressed executive and regulatory support for flexibility/openness to novel/innovative business models, including:

- De novo banks focused on digital assets.
- Non-financial companies to issue payment stablecoins.
- Fintechs and crypto-native companies obtaining a Federal Reserve master account.

### Examples

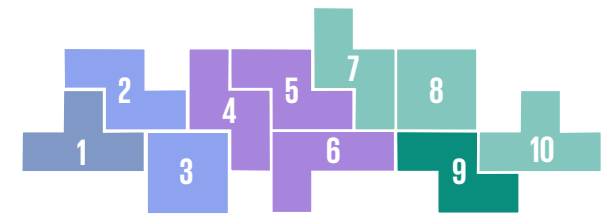
- OCC preliminary approval of de novo bank charter focused on digital assets
- “Permitted Payment Stablecoin Issuer” as defined and subject to forthcoming licensing regulations from federal or state regulators (e.g., P.L. 119-27, the GENIUS Act)
- Public remarks on “embracing new technologies and players in payments” (e.g., FRB (Waller), FRB Payments Innovation Conference)

### What to Watch

- Proliferation of new charter applications for stablecoin issuers and digital asset custodians at federal and state levels
- Increasing numbers of bank/fintech arrangements/acquisitions
- New and amended rules to permit novel/innovative products and business models, including:
  - On-chain software systems/decentralized finance
  - Non-securities trading authorities for SEC registrants
  - Consideration of a “skinny master account” at the Federal Reserve for certain bank and nonbank payment companies



# 09 Expanding Digital Assets



## Regulatory Signals

- Frameworks
- Risk Considerations
- Licensing/Chartering
- Access

### Signal

Executive directives to expand customer/investor access to alternative assets, including digital assets, through:

- Retail investor access to alternative asset investments in ERISA plans.
- Regulatory changes to encourage market participation (e.g., “self-custody,” “super-app” trading) and/or promote capital formation (e.g., accredited investor qualifications).

### Examples

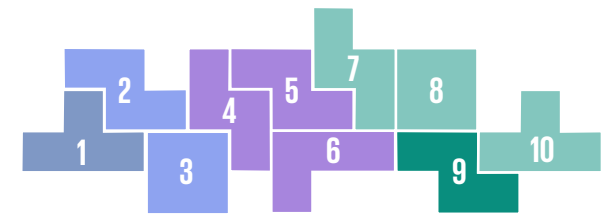
- Policy to permit retirement plan fiduciaries to permit retail investors to access alternative assets, including private funds and commodities (e.g., EO 14330)
- Recission of guidance directing ERISA plan fiduciaries to use “extreme care” when adding cryptocurrencies to an investment menu (e.g., DOL recission of Compliance Assistance Release No. 2022-01)
- Consideration of expanding access to private assets to retail investors (e.g., SEC Statements (Atkins, Uyeda))

### What to Watch

- DOL proposed rules/regulations/guidance on fiduciary duty when recommending investments in alternative assets in ERISA plans (anticipated 1st quarter 2026)
- Possible legislation or SEC rulemaking to amend definitions for accredited investor and qualified purchaser
- Expanded markets for tokenized assets (e.g., tokenized collateral in derivatives markets)



# 09 Expanding Digital Assets



## Regulatory Signals

- Frameworks
- Risk Considerations
- Licensing/Chartering
- Access

## Relevant Thought Leadership



[Stablecoins: The bridge between traditional finance and digital assets](#)



[KPMG digital assets – Financial services](#)



[Digital assets and blockchain technology](#)

## Top Related Regulatory Challenges

[01 Executing Mandates](#)

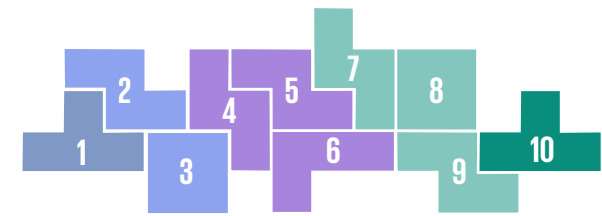
[02 Adopting Disruptive Tech & AI](#)

[04 Mitigating Financial Crimes](#)

[08 Driving Capital Formation & Growth](#)



# 10 Enhancing Parties & Workforce



## Regulatory Signals

- Third-Party Risk Management
- Concentration Risk
- Dynamic Workforce
- Protecting Workers

*Third-Party Risk Management remains a focus of regulators, highlighting oversight of the full lifecycle of third-party relationships, especially critical service providers. Concurrently, employing a skilled workforce is a critical element for both regulators and organizations.*

*“Business leaders are now leveraging worker’s safety as a competitive edge, moving beyond compliance to make critical investments in their workforce that foster resilience, build trust, and drive business success.”*



**Kirk Caron**  
Managing Director  
Advisory

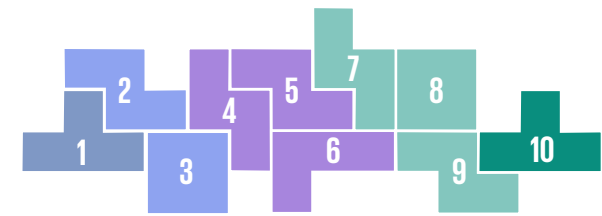
*“Dependence upon third-/fourth-party providers has become entrenched in most companies’ business models, elevating operational risk (non-financial risk) as well as regulatory scrutiny. Regulators expect companies to enhance third-/fourth-party governance, processes, and technology use to reduce risk, streamline operations, expand coverage , and strengthen resiliency.”*



**Joey Gyengo**  
Principal  
Advisory



# 10 Enhancing Parties & Workforce



## Regulatory Signals

- **Third-Party Risk Management**
- Concentration Risk
- Dynamic Workforce
- Protecting Workers

### Signal

Continued focus on the full lifecycle of the relationship with third parties including initial due diligence, contract negotiation, ongoing monitoring and oversight, and termination. Oversight extends to fourth parties and beyond, including potential re-assessment to accommodate sanctions and tariffs.

### Examples

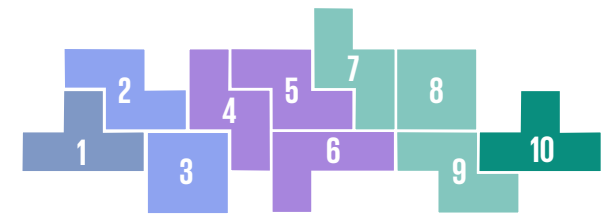
- Guidance on managing third-party risks (e.g., NYDFS Industry Letter)
- Dedicated oversight category in 2025 to “Third-Party Risk Landscape” (i.e., FINRA 2025 Annual Regulatory Oversight Report)
- Enforcement actions focused on consumer harm and lack of due diligence of third parties (e.g., FTC)

### What to Watch

- Potential geopolitical impacts (e.g., tariffs and sanctions) will require visibility into third-party/vendor chains
- Demands for a comprehensive and proactive approach to third parties, integrated across the enterprise, and potentially folded into enterprise risk management
- Enforcement priorities on third-party liability, including data privacy/data collection, consumer protection and due diligence



# 10 Enhancing Parties & Workforce



## Regulatory Signals

- Third-Party Risk Management
- Concentration Risk
- Dynamic Workforce
- Protecting Workers

### Signal

Increasing reliance on third parties, and in many cases a small number of the same third parties, increases risk (e.g., financial stability, contagion) requiring ongoing assessment and monitoring, especially those supporting an entity's critical services. Third parties may allow for a single point of failure or create systemic vulnerabilities.

### Examples

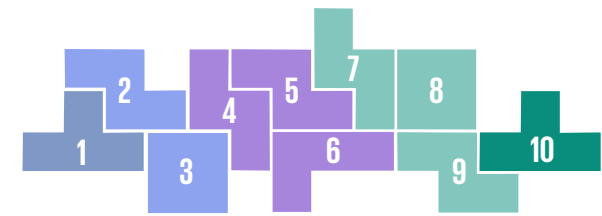
- Technology-focused third parties and impact to financial institutions and the market (e.g., Federal Reserve Bank of Boston, Chicago and Dallas Paper)
- Requirement for sound third-party risk management (e.g., OCC Spring 2025 Semiannual Risk Perspective)
- Limited number of providers for critical infrastructure services introduces risk management concerns (e.g., CFTC 2025 Regulators Roundtable)
- Creation of an interagency technology service provider supervision program to assist banks with their ongoing monitoring of third-party risk (e.g., FRB Cybersecurity and Financial System Resilience Report)

### What to Watch

- Increased interconnectedness between financial institutions and dependency on third parties due to limited numbers of service providers in certain spaces such as AI and cloud services



# 10 Enhancing Parties & Workforce



## Regulatory Signals

- Third-Party Risk Management
- Concentration Risk
- Dynamic Workforce
- Protecting Workers

### Signal

Balancing the Administration’s federal reductions in force initiatives with the need for experienced and knowledgeable regulators to respond to emerging risks in technology, cybersecurity and digital assets. Complemented by industry emphasis to align employee training with employer needs.

### Examples

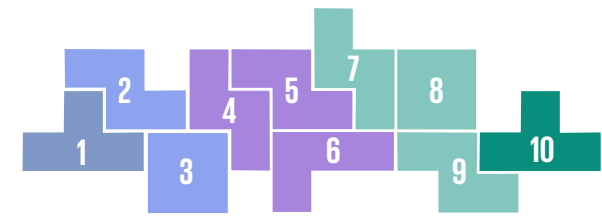
- Announced plans for workforce reductions in 2026 (e.g., FRB Statement (Bowman), SEC Statement (Atkins))
- Highlighting need for enhanced regulator’s expertise and skills (e.g., CFTC 2025 Regulators Roundtable)
- Building talent pipelines and workforce development (e.g., DOL America’s Talent Strategy Report, AI Action Plan)
- Federal agencies mass layoffs (e.g., Supreme Court ruling)

### What to Watch

- Continued reductions in force and reorganizations of federal agencies and regulators
- Continued shift of workforce from federal agencies to state agencies (e.g., more than 200,000 federal employees left the workforce in 2025), certain states implementing hiring campaigns to recruit laid-off federal workers
- Industry investment in continuous learning, shift towards skills-based hiring



# 10 Enhancing Parties & Workforce



## Regulatory Signals

- Third-Party Risk Management
- Concentration Risk
- Dynamic Workforce
- **Protecting Workers**

### Signal

Heightened attention to physical security and employee well-being through workplace safety laws. Focus on protecting employees from unfair or deceptive practices, including impacts of AI-driven workplace monitoring such as biometric surveillance.

### Examples

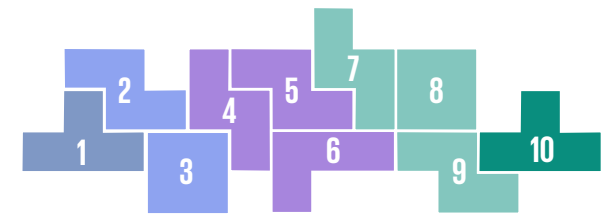
- Introduced legislation across states focused on workplace and psychological safety, including healthcare professionals, and heat safety standards
- Proposed modernization of workplace safety standards (e.g., OSHA proposed rule)
- Treatment of employees as consumers too, ensuring no unfair or deceptive practices (e.g., FTC Joint Labor Task Force)

### What to Watch

- States to continue to introduce workplace safety legislation, with a focus on public health and emerging safety risks (e.g., psychological safety, workplace violence prevention, heat hazard protections)
- Enforcement through data-driven inspection programs
- Focus on deceptive, unfair and anticompetitive labor-market practices (e.g., no-hire agreements, noncompete agreements)



# 10 Enhancing Parties & Workforce



## Regulatory Signals

- Third-Party Risk Management
- Concentration Risk
- Dynamic Workforce
- Protecting Workers

## Relevant Thought Leadership



[The partner paradox: How to thrive in an evolving risk landscape](#)



[Renewed Urgency on Third Party Risk Management](#)

## Top Related Regulatory Challenges

[02 Adopting Disruptive Tech & AI](#)

[06 Protecting Fairness](#)

[03 Maintaining Cyber & Data Security](#)

[08 Driving Capital Formation & Growth](#)

[04 Mitigating Financial Crimes](#)



# KPMG Regulatory Insights

KPMG [Regulatory Insights](#) is the thought leader hub for timely insight on risk and regulatory developments. Our perspectives enable our clients to help anticipate and manage regulatory change across the U.S. regulatory landscape. In collaboration with professionals across the firm's global regulatory practices, we provide perspectives on emerging regulatory and enforcement risks, and insight on actions as they occur.



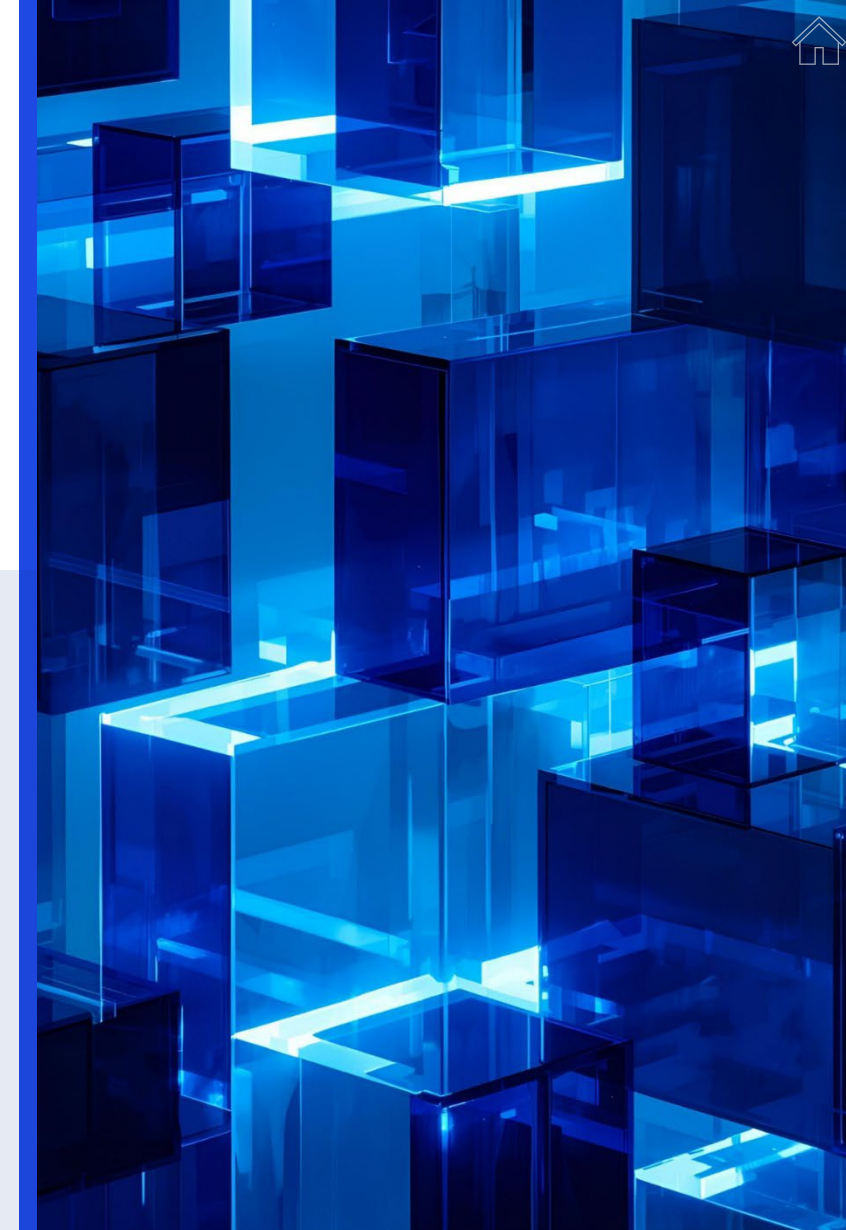
## Regulatory Alerts

Quick hitting summaries of specific regulatory developments and their impact on businesses across industries.



## Points of View

Insights and analyses of emerging regulatory issues impacting businesses across industries.

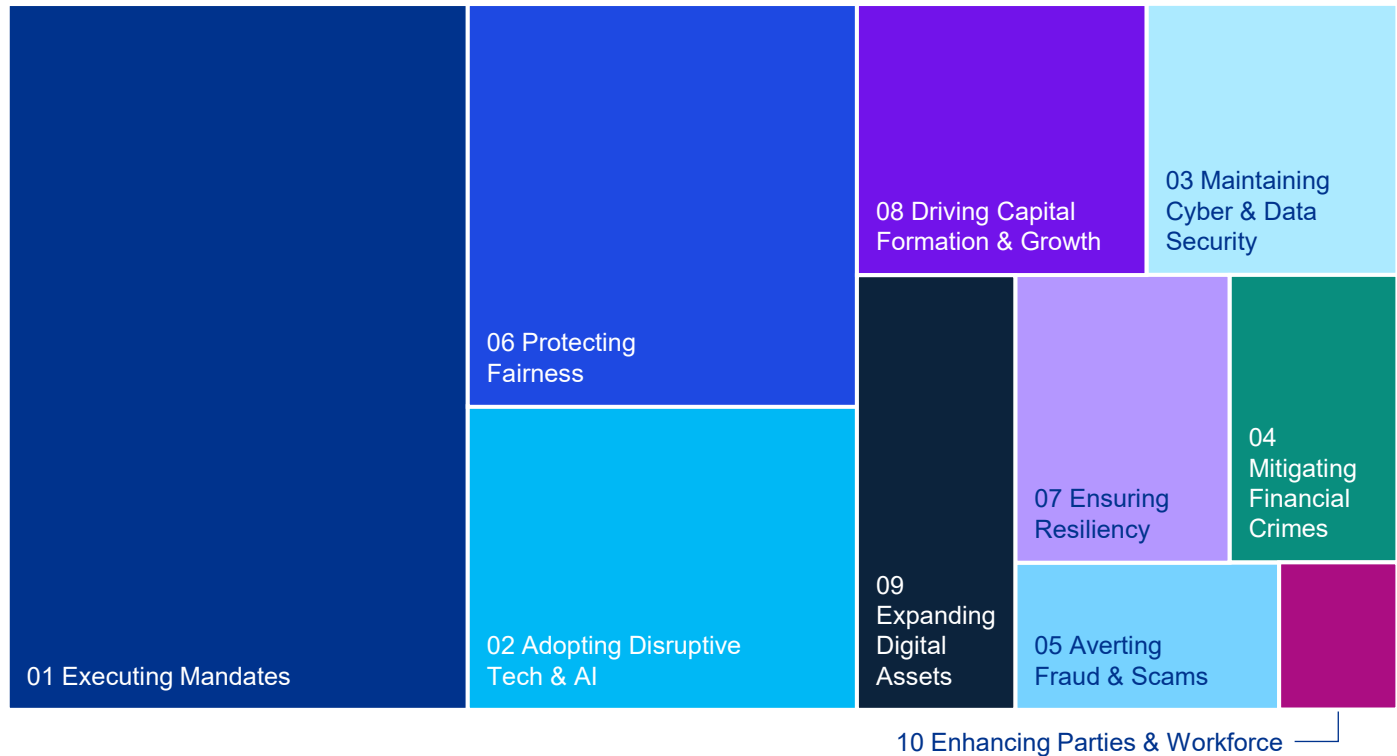




# Regulatory Analytics

On an ongoing basis, KPMG Regulatory Insights monitors and tracks cross-industry public policy and regulatory activity at the federal and state levels, including executive orders, legislation, Congressional hearings, rulemakings, guidance, speeches, and related news articles. Using text analytics, we have classified these items into predetermined topics—in this case, the Ten Key Regulatory Challenges of 2026.

This year, with the change in Administration and related regulatory priorities, we have limited our analysis to items monitored between January 2025 and September 2025. This graph visually represents the number of records in each of the ten key challenge areas.





# List of Acronyms

ACH	Automated Clearing House	CIP	Customer Identification Program	DOL	Department of Labor
ADI	Advisor-Directed Investing	CISA	Cybersecurity and Infrastructure Security Agency	DORA	Digital Operational Resilience Act
AG	Attorney General	CISA 2015	Cybersecurity Information Sharing Act of 2015	DPDPA	Digital Personal Data Protection Act
AI	Artificial Intelligence	CLARITY	Creating Legal Accountability for Regulators in the Treatment of Your Assets	DPF	Data Privacy Framework
AML	Anti-Money Laundering	CMMC	Cybersecurity Maturity Model Certification	ECOA	Equal Credit Opportunity Act
API	Application Programming Interfaces	COPPA	Children's Online Privacy Protection Act	EO	Executive Order
BDC	Business Development Company	CRI	Cyber Risk Institute	EPA	Environmental Protection Agency
BOI	Beneficial Ownership Interest	CSC	Cyberspace Solarium Commission	ERISA	Employee Retirement Income Security Act
BSA	Bank Secrecy Act	CTA	Corporate Transparency Act	ESLR	Enhanced Supplementary Leverage Ratio
CBLR	Community Bank Leverage Ratio	CTR	Currency Transaction Report	EU	European Union
CCPA	California Consumer Privacy Act	DEI	Diversity, Equity, and Inclusion	FAQ	Frequently Asked Question
CECL	Current Expected Credit Losses	DHS	Department of Homeland Security	FBI	Federal Bureau of Investigation
CFPB	Consumer Financial Protection Bureau	DOC	Department of Commerce	FCA	False Claims Act
CFT	Combating the Financing of Terrorism	DOD	Department of Defense	FCC	Federal Communications Commission
CFTC	Commodity Futures Trading Commission	DOJ	Department of Justice	FCPA	Foreign Corrupt Practices Act



# List of Acronyms (continued)

FDIC	Federal Deposit Insurance Corporation	IC3	Internet Crime Complaint Center	ONCD	Office of the National Cyber Director
FFIEC	Federal Financial Institutions Examination Council	ICT	Information and Communications Technology	OSHA	Occupational Safety and Health Administration
FHA	Fair Housing Act	ILC	Industrial Loan Company	OSTP	Office of Science and Technology Policy
FHLB	Federal Home Loan Bank	IPO	Initial Public Offering	PD	Private Debt
FINRA	Financial Industry Regulatory Authority	IT	Information Technology	PF	Private Fund
FinCEN	Financial Crimes Enforcement Network	M&A	Mergers and Acquisitions	P.L.	Public Law
FMU	Financial Market Utility	NACHA	National Automated Clearing House Association	PWG	President's Working Group
FRB	Federal Reserve Board	NCSL	National Conference of State Legislatures	RFI	Request for Information
FSOC	Financial Stability Oversight Council	NCUA	National Credit Union Administration	RIA	Registered Investment Advisors
FTC	Federal Trade Commission	NDFI	Non-Depository Financial Institution	SAR	Suspicious Activity Report
GAO	Government Accountability Office	NIH	National Institutes of Health	SDN	Specially Designated Nationals
GDPR	General Data Protection Regulation	NIST	National Institute of Standards and Technology	SEC	Securities and Exchange Commission
GENIUS	Guiding and Establishing National Innovation for US Stablecoins	NYDFS	New York Department of Financial Services	SR	Supervision and Regulation Letters
GenAI	Generative Artificial Intelligence	OCC	Office of the Comptroller of the Currency	TCO	Transnational Criminal Organizations
HSR	Hart-Scott-Rodino	OFAC	Office of Foreign Assets Control	TPRM	Third-Party Risk Management



# List of Executive Orders

EO 14151	Ending Radical and Wasteful Government DEI Programs and Preferencing
EO 14154	Unleashing American Energy
EO 14157	Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists
EO 14161	Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats
EO 14178	Strengthening American Leadership in Digital Financial Technology
EO 14219	Ensuring Lawful Governance and Implementing the President's "Department of Government Efficiency" Deregulatory Initiative
EO 14239	Achieving Efficiency Through State and Local Preparedness
EO 14243	Stopping Waste, Fraud, and Abuse by Eliminating Information Silos
EO 14254	Combating Unfair Practices in the Live Entertainment Market
EO 14260	Protecting American Energy From State Overreach
EO 14281	Restoring Equality of Opportunity and Meritocracy
EO 14297	Delivering Most-Favored-Nation Prescription Drug Pricing to American Patients
EO 14306	Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144
EO 14318	Accelerating Federal Permitting of Data Center Infrastructure
EO 14320	Promoting the Export of the American AI Technology Stack
EO 14330	Democratizing Access to Alternative Assets for 401(k) Investors
EO 14331	Guaranteeing Fair Banking for All Americans

# Contact



**Laura Byerly**

**Managing Director**  
KPMG Regulatory Insights

[lbyerly@kpmg.com](mailto:lbyerly@kpmg.com)  
[LinkedIn](#)

<p><b>01 Executing Mandates</b></p> <p><b>Laura Byerly</b> <a href="mailto:lbyerly@kpmg.com">lbyerly@kpmg.com</a> <a href="#">LinkedIn</a></p>	<p><b>02 Adopting Disruptive Tech &amp; AI</b></p> <p><b>Adam Levy</b> <a href="mailto:adamlevy@kpmg.com">adamlevy@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Bryan McGowan</b> <a href="mailto:bmcgowan@kpmg.com">bmcgowan@kpmg.com</a> <a href="#">LinkedIn</a></p>	<p><b>03 Maintaining Cyber &amp; Data Security</b></p> <p><b>Orson Lucas</b> <a href="mailto:olucas@kpmg.com">olucas@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Matt Miller</b> <a href="mailto:matthewpmiller@kpmg.com">matthewpmiller@kpmg.com</a> <a href="#">LinkedIn</a></p>	<p><b>04 Mitigating Financial Crimes</b></p> <p><b>Steve D'Antuono</b> <a href="mailto:sdantuono@KPMG.com">sdantuono@KPMG.com</a> <a href="#">LinkedIn</a></p> <p><b>Chad Polen</b> <a href="mailto:cpolen@kpmg.com">cpolen@kpmg.com</a> <a href="#">LinkedIn</a></p>	<p><b>05 Averting Fraud &amp; Scams</b></p> <p><b>John Caruso</b> <a href="mailto:johncaruso@kpmg.com">johncaruso@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>DJ Hennes</b> <a href="mailto:dhennes@kpmg.com">dhennes@kpmg.com</a> <a href="#">LinkedIn</a></p>
<p><b>06 Protecting Fairness</b></p> <p><b>Mike Lamberth</b> <a href="mailto:mlamberth@kpmg.com">mlamberth@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Mike Sullivan</b> <a href="mailto:mmsullivan@KPMG.com">mmsullivan@KPMG.com</a> <a href="#">LinkedIn</a></p>	<p><b>07 Ensuring Resiliency</b></p> <p><b>KB Babar</b> <a href="mailto:kbabar@kpmg.com">kbabar@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Prince Harfouche</b> <a href="mailto:pharfouche@kpmg.com">pharfouche@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>David Tarabocchia</b> <a href="mailto:dtarabocchia@kpmg.com">dtarabocchia@kpmg.com</a> <a href="#">LinkedIn</a></p>	<p><b>08 Driving Capital Formation &amp; Growth</b></p> <p><b>Henry Lacey</b> <a href="mailto:hlacey@kpmg.com">hlacey@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Nadia Orawski</b> <a href="mailto:norawski@kpmg.com">norawski@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Mike Sullivan</b> <a href="mailto:mmsullivan@KPMG.com">mmsullivan@KPMG.com</a> <a href="#">LinkedIn</a></p>	<p><b>09 Expanding Digital Assets</b></p> <p><b>Brian Consolvo</b> <a href="mailto:bconsolvo@kpmg.com">bconsolvo@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Conway Dodge</b> <a href="mailto:conwaydodge@kpmg.com">conwaydodge@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Todd Semanco</b> <a href="mailto:tsemanco@kpmg.com">tsemanco@kpmg.com</a> <a href="#">LinkedIn</a></p>	<p><b>10 Enhancing Parties &amp; Workforce</b></p> <p><b>Kirk Caron</b> <a href="mailto:kcaron@kpmg.com">kcaron@kpmg.com</a> <a href="#">LinkedIn</a></p> <p><b>Joey Gyengo</b> <a href="mailto:jgyengo@kpmg.com">jgyengo@kpmg.com</a> <a href="#">LinkedIn</a></p>



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us:



[kpmg.com](https://kpmg.com)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.