IIA Atlanta Chapter Meeting hosted by KPMG

Thursday, June 26

June 2025
Chapter Meeting

Welcome to the IIA Atlanta June Chapter Meeting

Our thanks to KPMG for their support and development of the meeting this morning.

KPMG

The Institute of
Internal Auditors

Agenda

9:00AM	**Meeting Opens**
9:00 – 9:10AM	Announcements **Thomas Sherrill – President, IIA Atlanta**
9:10 – 10:00AM	Global Economy Update **Ben Shoesmith – Senior Economist, Director, KPMG LLP**
10:00 – 11:00AM	Third-Party Risk Management **Michael Bruner, Managing Director, KPMG LLP** **Kyle Thompson, Director, KPMG LLP**

Newly-certified members

April – May 2025

Certified Internal Auditor®

Doreen Tetteh
William Meira
Brittany Mosteller
Meredith Joy Franklin
Desiree Swagten
Connor Jackson
Thalya Rodriguez Vazquez
Tisha Millett
Shannan Phillips
Richard Rose
Lawrence King

Internal Audit Practitioner

Teia Deshun Carr
Christine Moore
Christopher Todaro

Narrowly averting recession: Decoupling, de-escalation and weathering storms

Business investment slackens.

Ben Shoesmith
Senior Economist

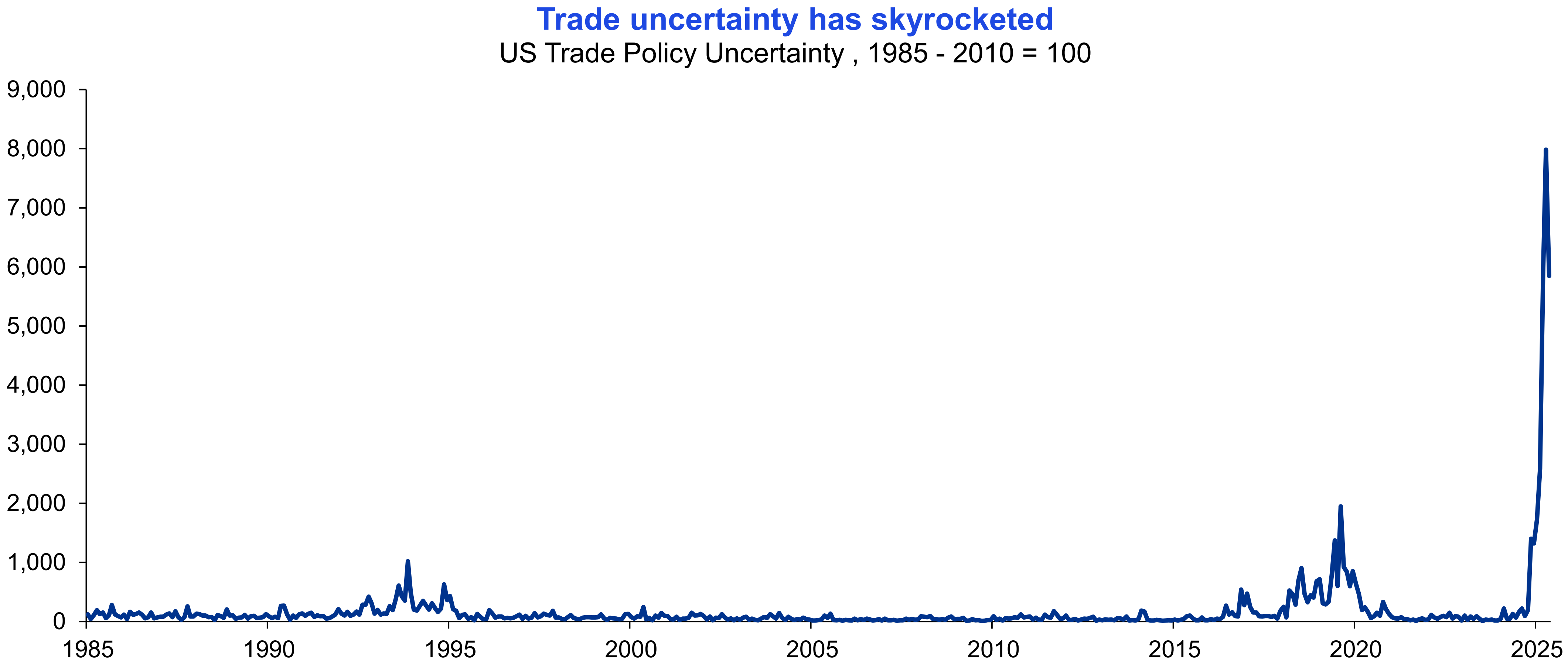
June 26, 2025

Agenda

01

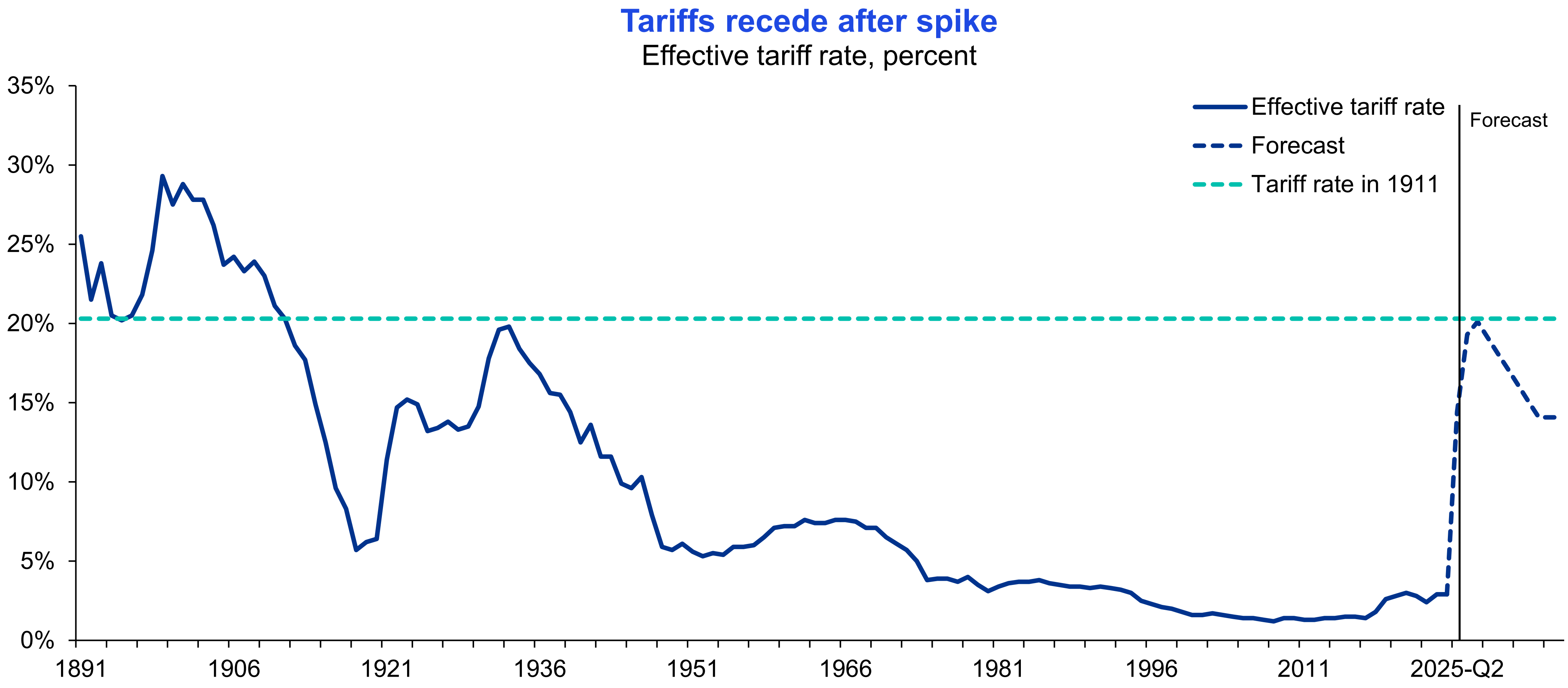
Trade

Policy uncertainty weighs on investment



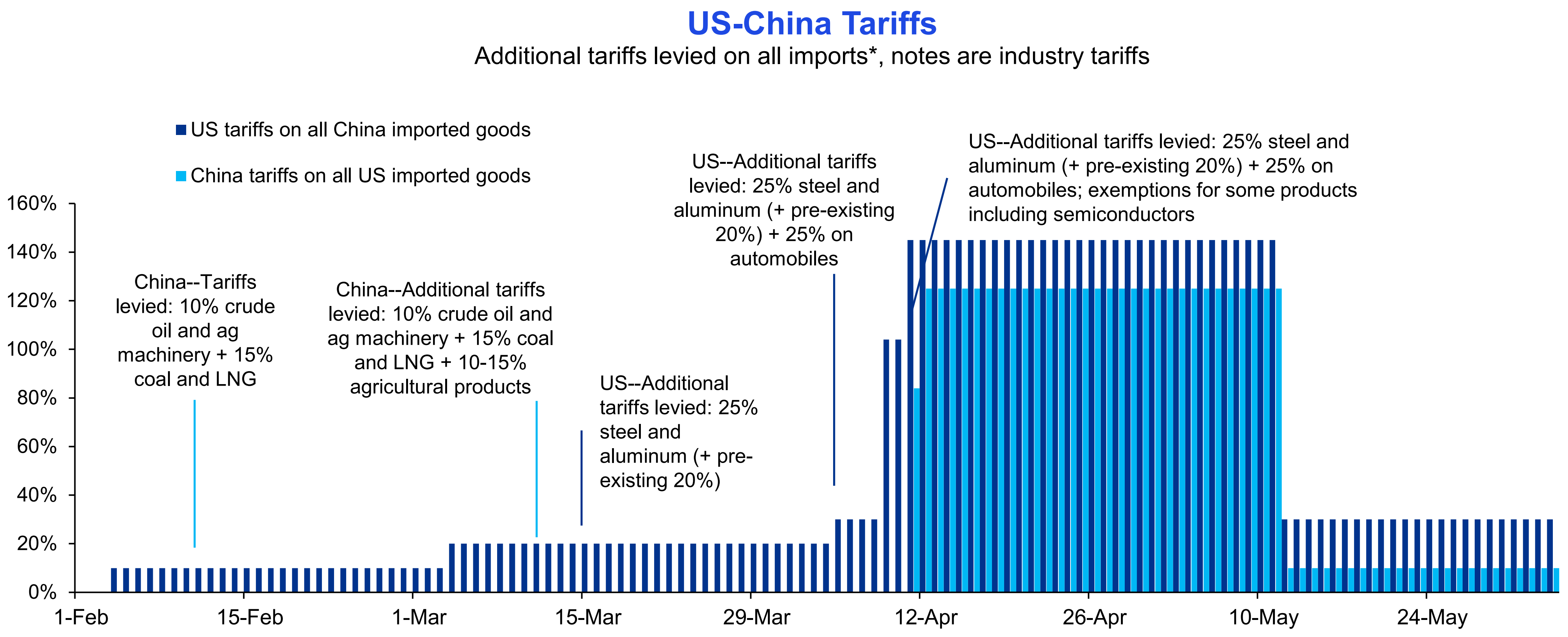
Source: KPMG Economics, PolicyUncertainty.com, Haver Analytics

Tariffs peak at highest level since the early 1900s



Source: KPMG Economics, United States Census Bureau

US-China tensions remain

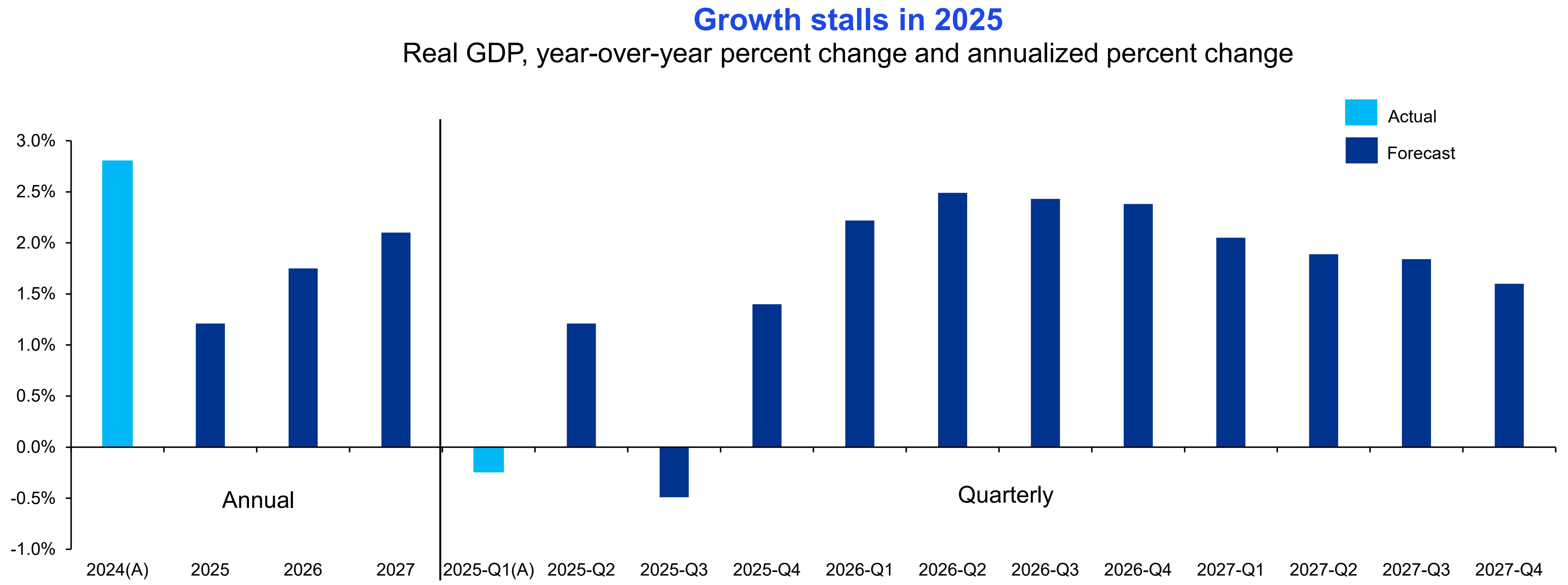


*As of June 3, 2025
Source: KPMG Economics

02

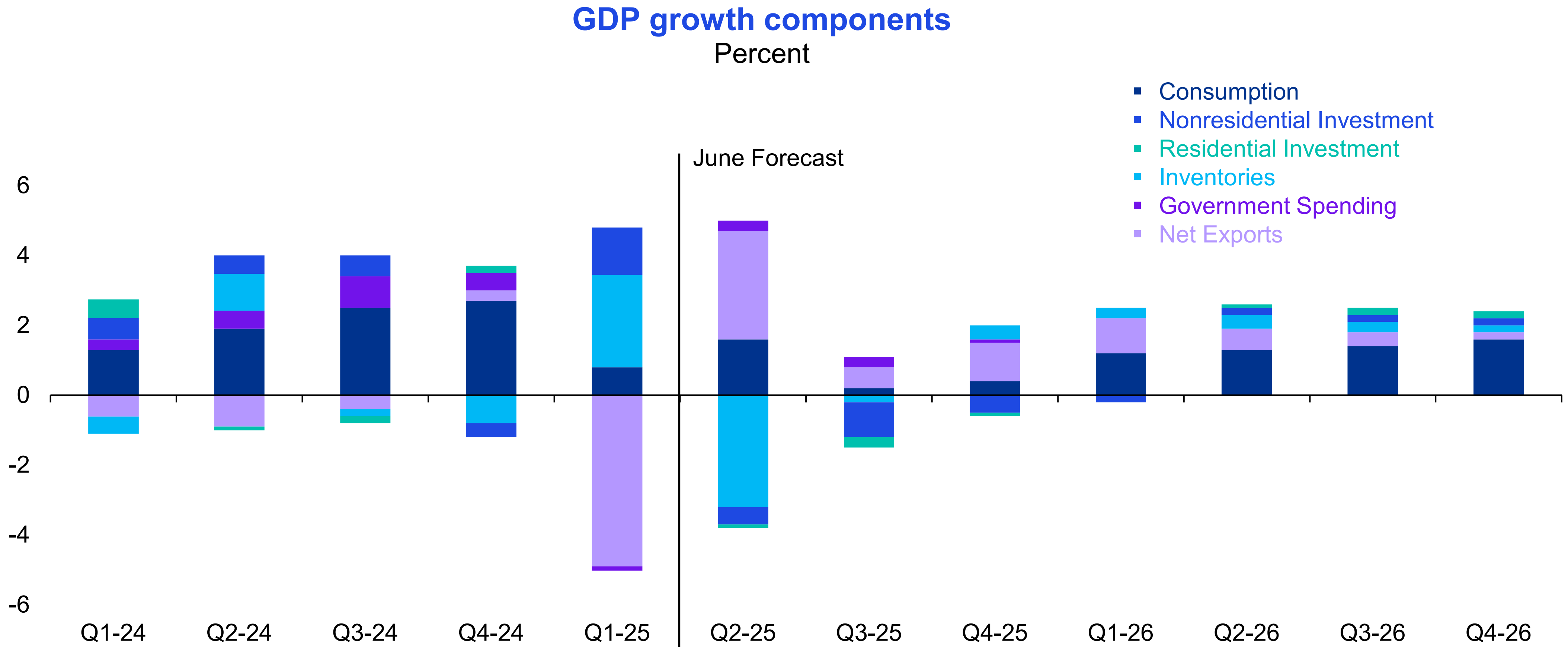
US Economy

Growth sputters throughout 2025



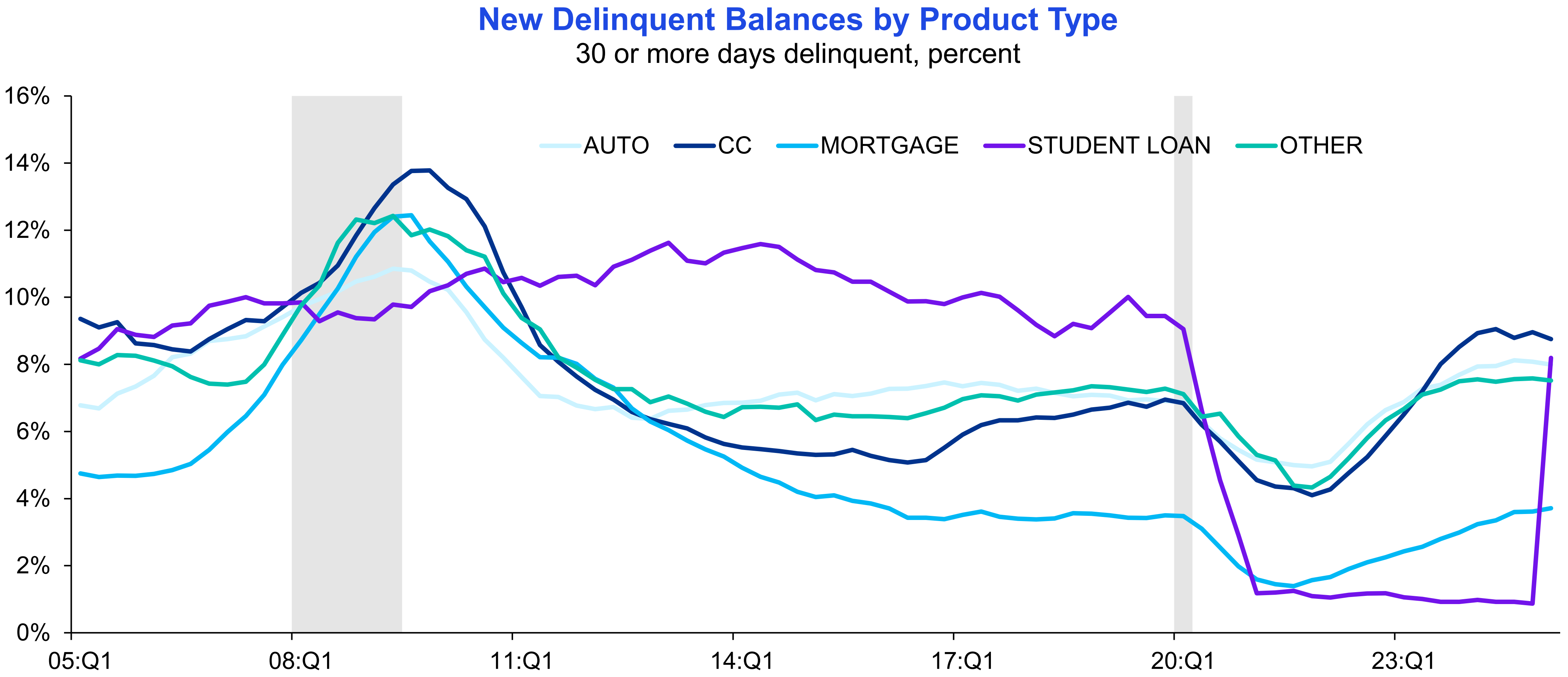
Source: KPMG Economics, Bureau of Economic Analysis

GDP swings on net exports



Source: KPMG Economics, Bureau of Economic Analysis

Most delinquencies above pre-pandemic rates



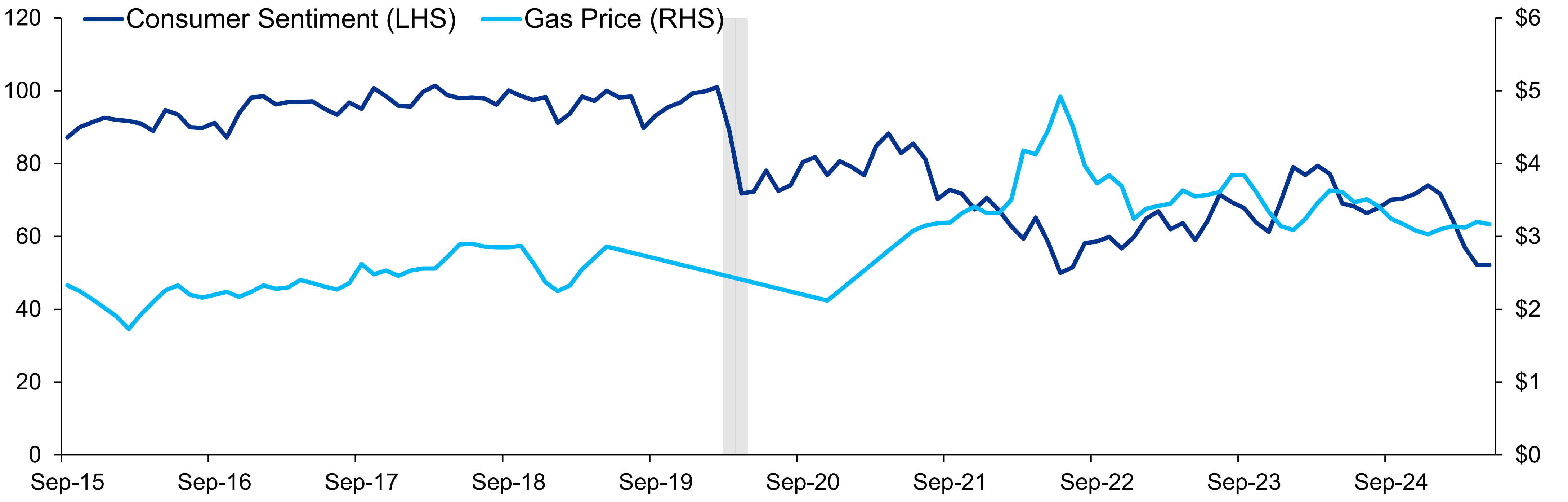
Source: KPMG Economics, New York Fed Consumer Credit Panel/Equifax

Price at the pump drives sentiment… and so do egg prices

Inverse relationship between consumer sentiment and gas prices

University of Michigan Consumer Sentiment: 1966 = 100, NSA

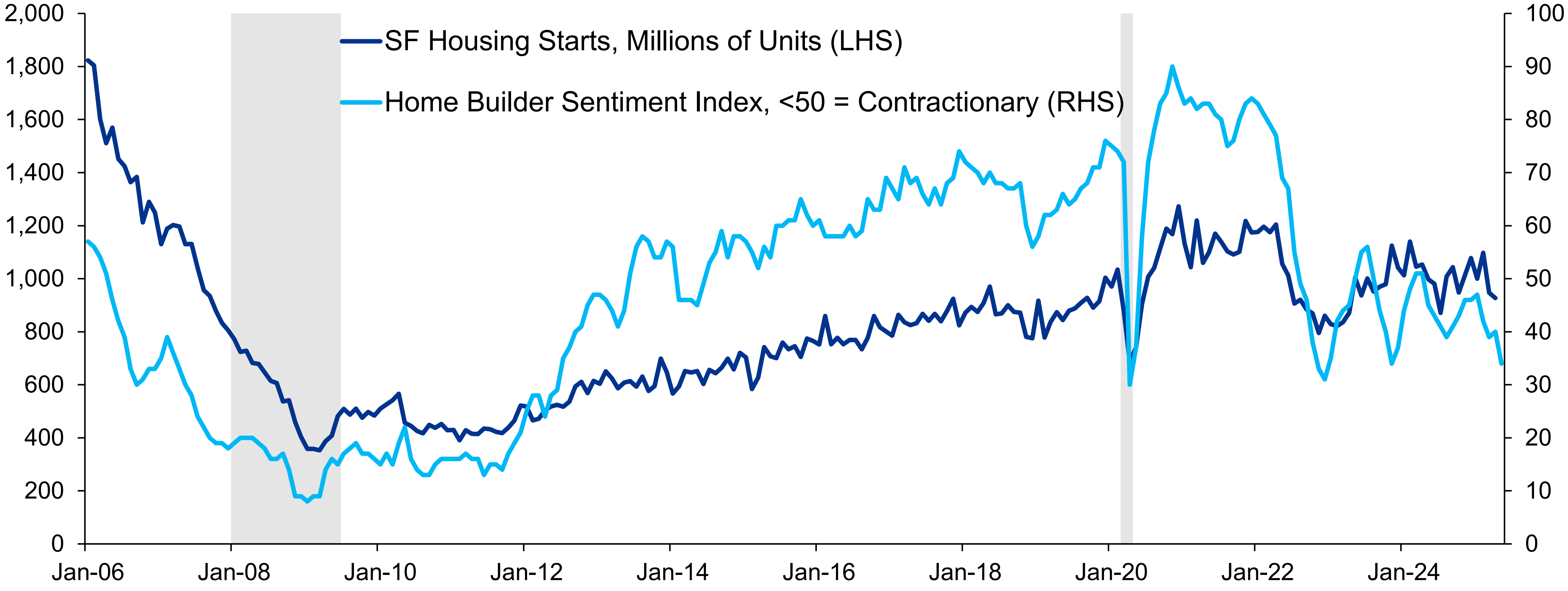
Gas: Average price per gallon



Source: KPMG Economics, University of Michigan, Bureau of Labor Statistics, Haver

Residential investment is still struggling

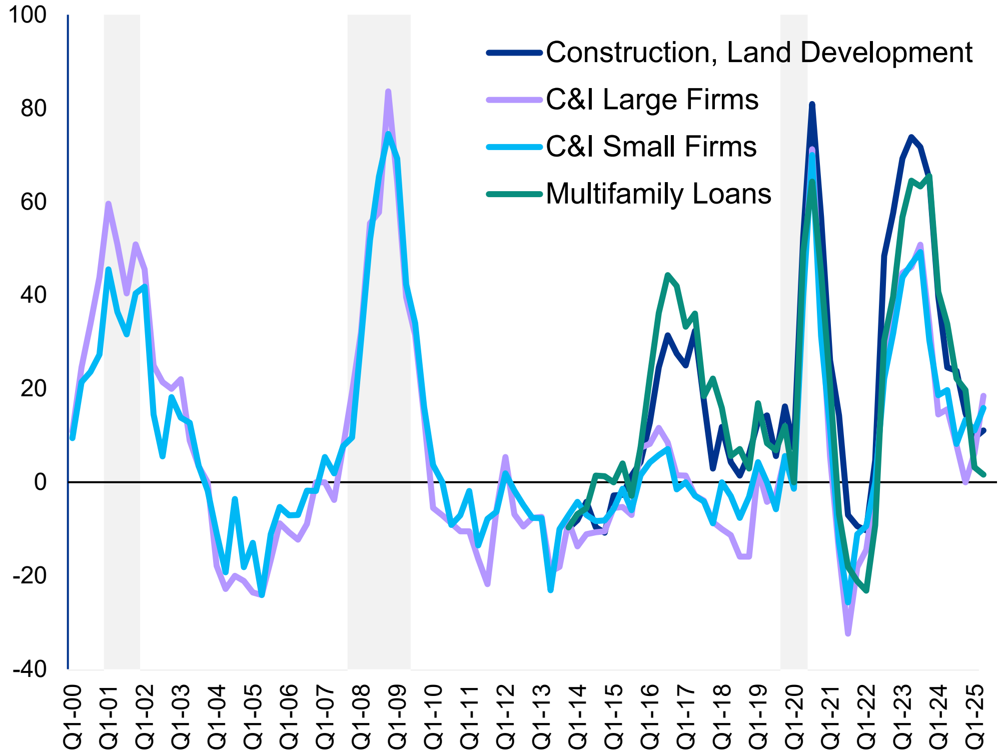
Homebuilder sentiment remains weak



Source: KPMG Economics, NAHB/WF, Census Bureau

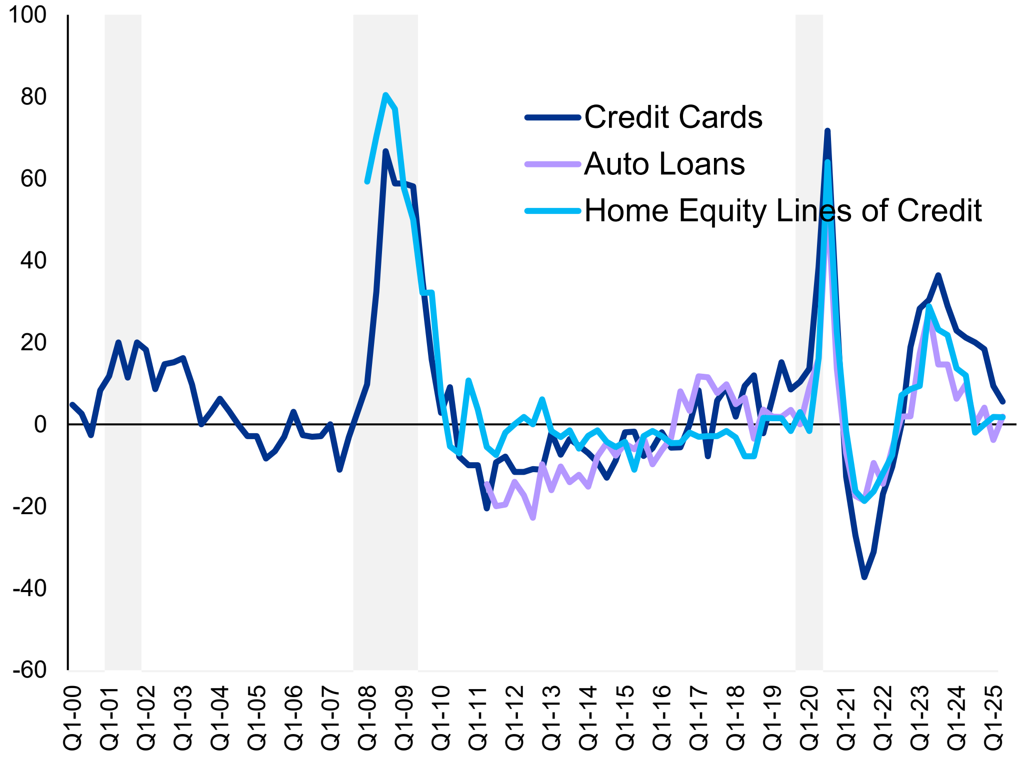
Lending conditions tightened in Q1

Tightening peaked in mid-2023
Percentage of banks reporting tightening standards



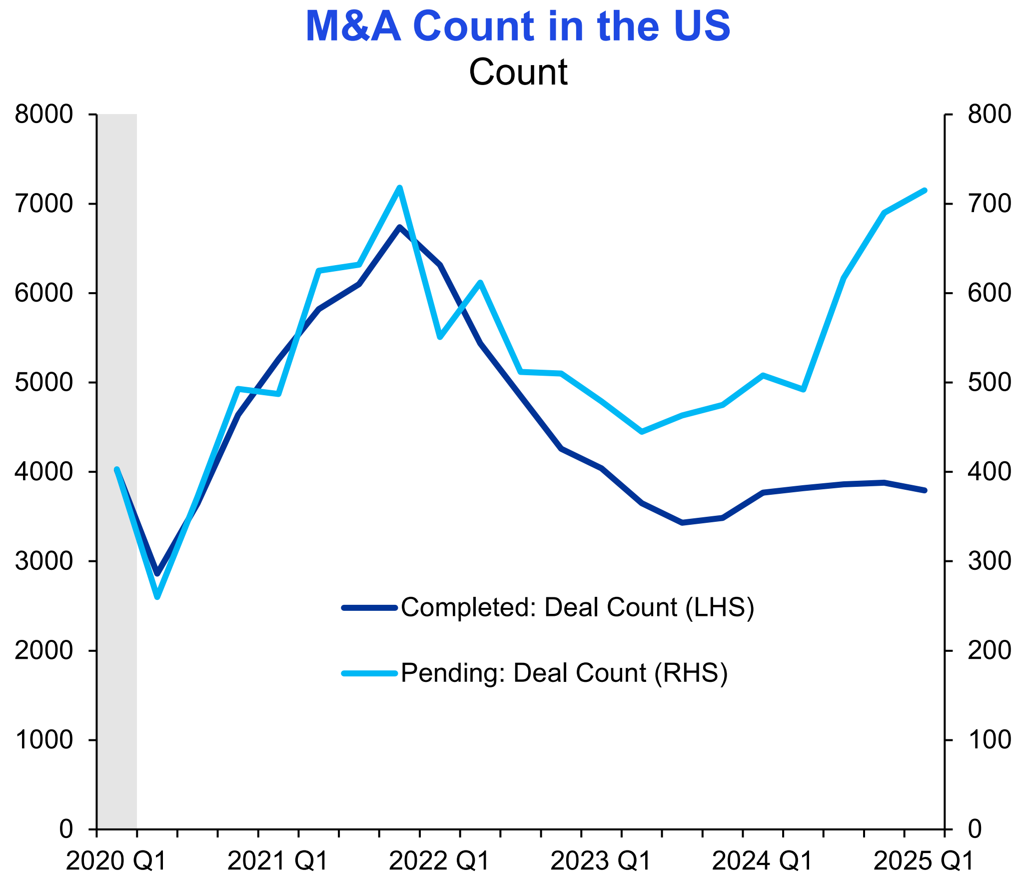
Source : KPMG Economics, BLS, Federal Reserve Board (Q4 2024), Haver Analytics

Tightening peaked in mid-2023
Percentage of banks reporting tightening standards

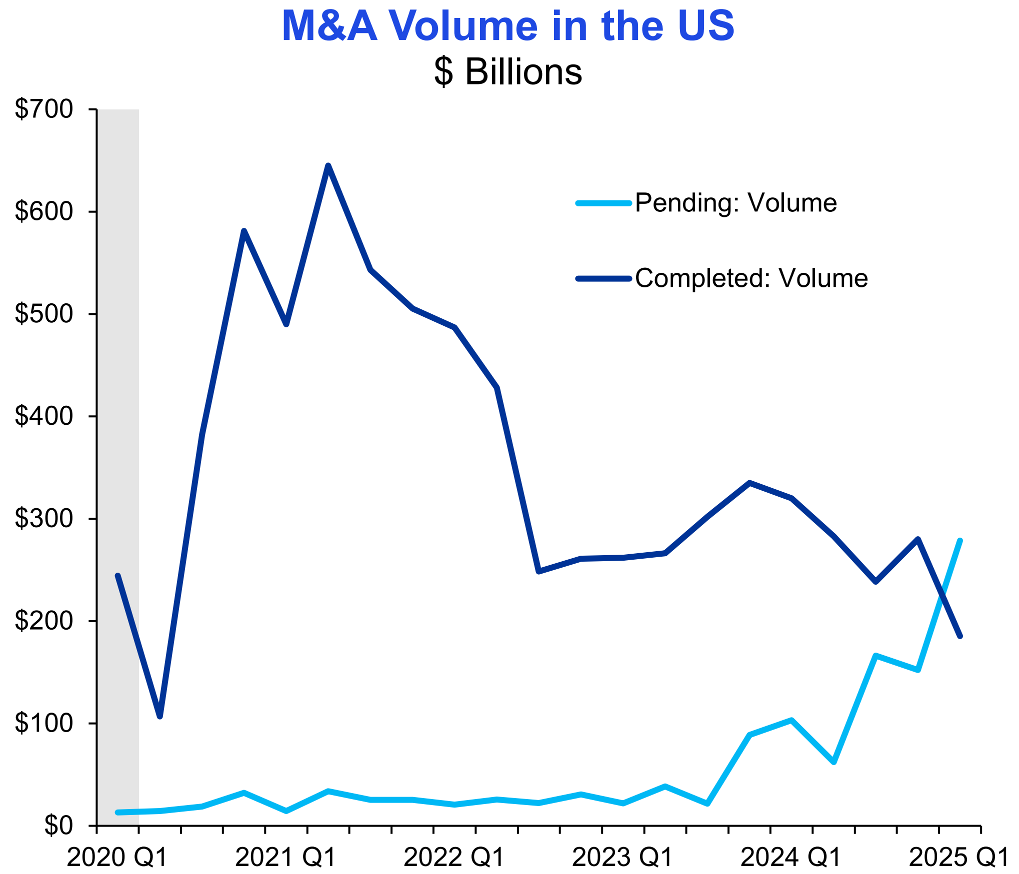


Source : KPMG Economics, BLS, Federal Reserve Board (Q4 2024), Haver Analytics

M&A activity has stalled

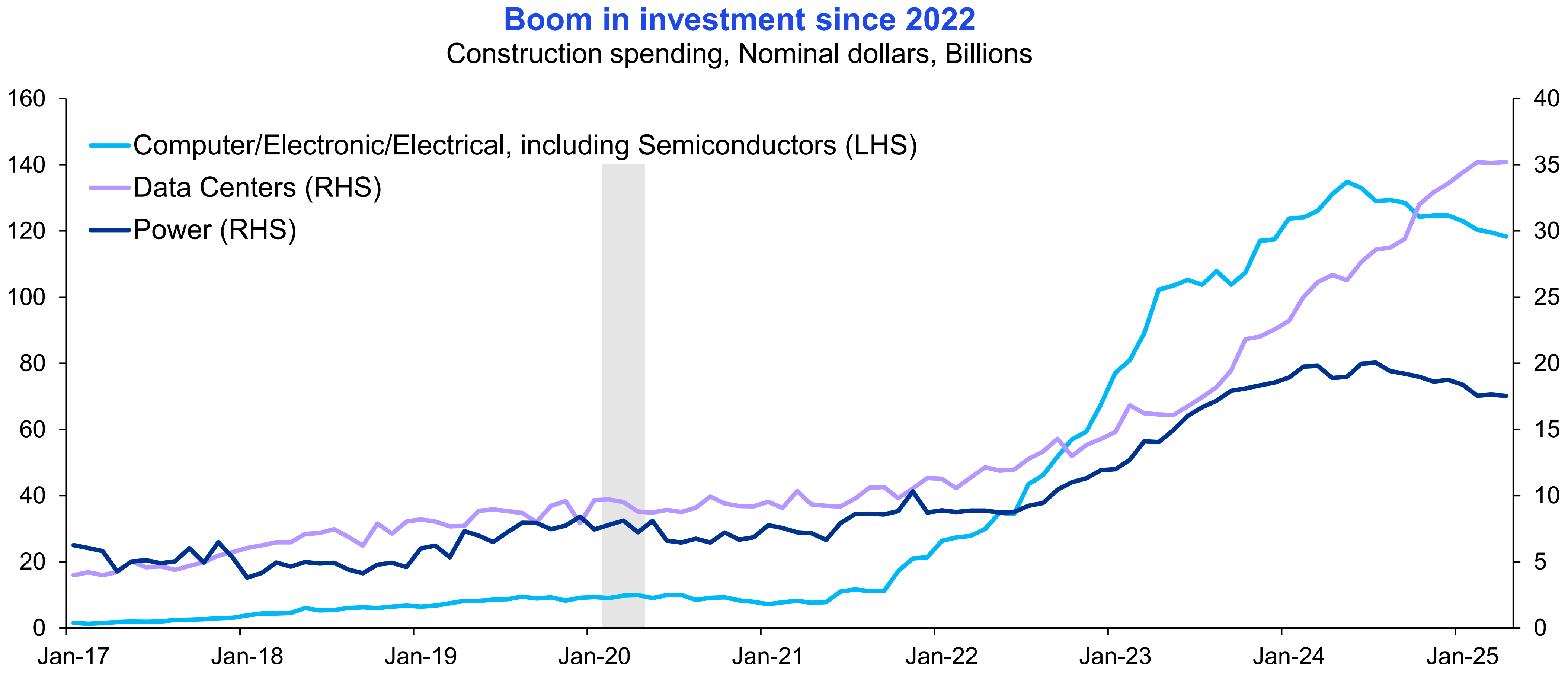


Source: KPMG Economics, Bloomberg



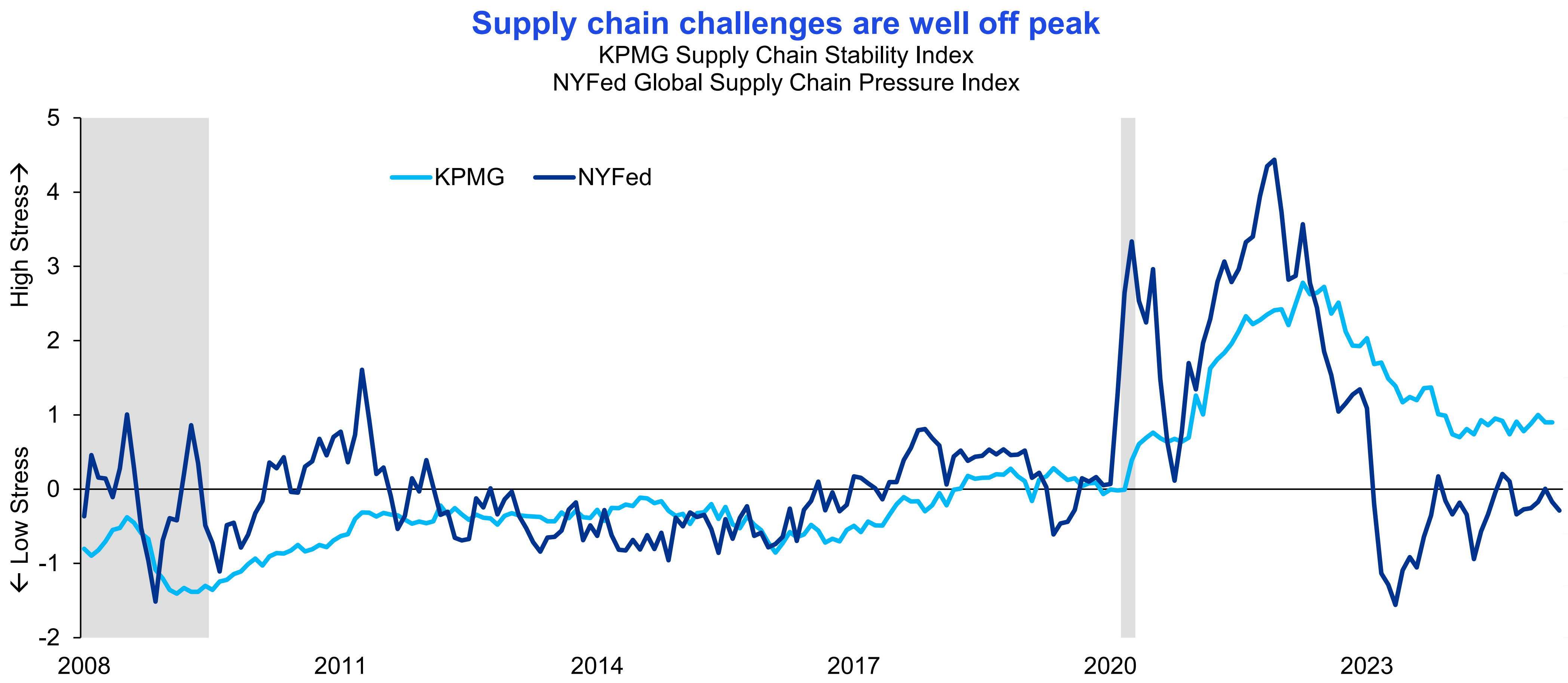
Source: KPMG Economics, Bloomberg

Construction boom for cooling for semiconductors and power



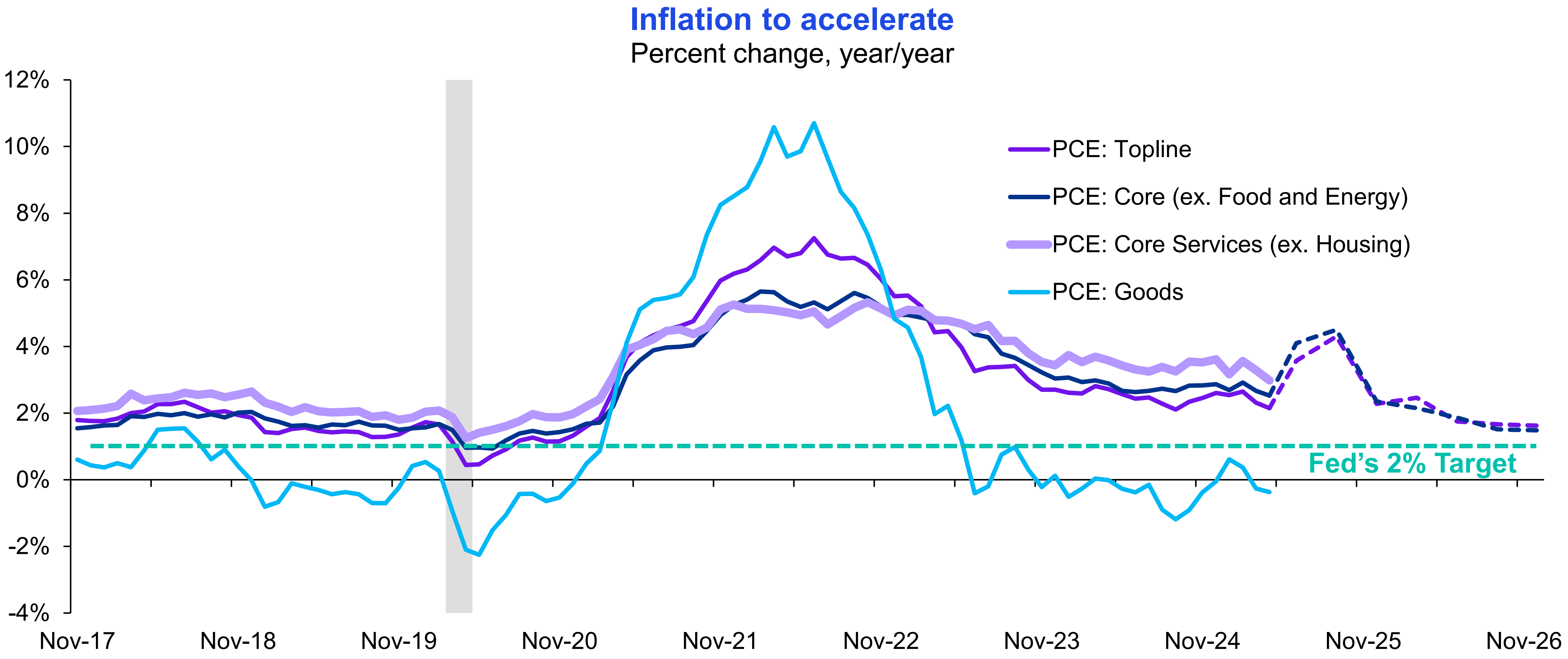
Source: KPMG Economics, Census Bureau, Haver Analytics

Supply chain stress likely to increase



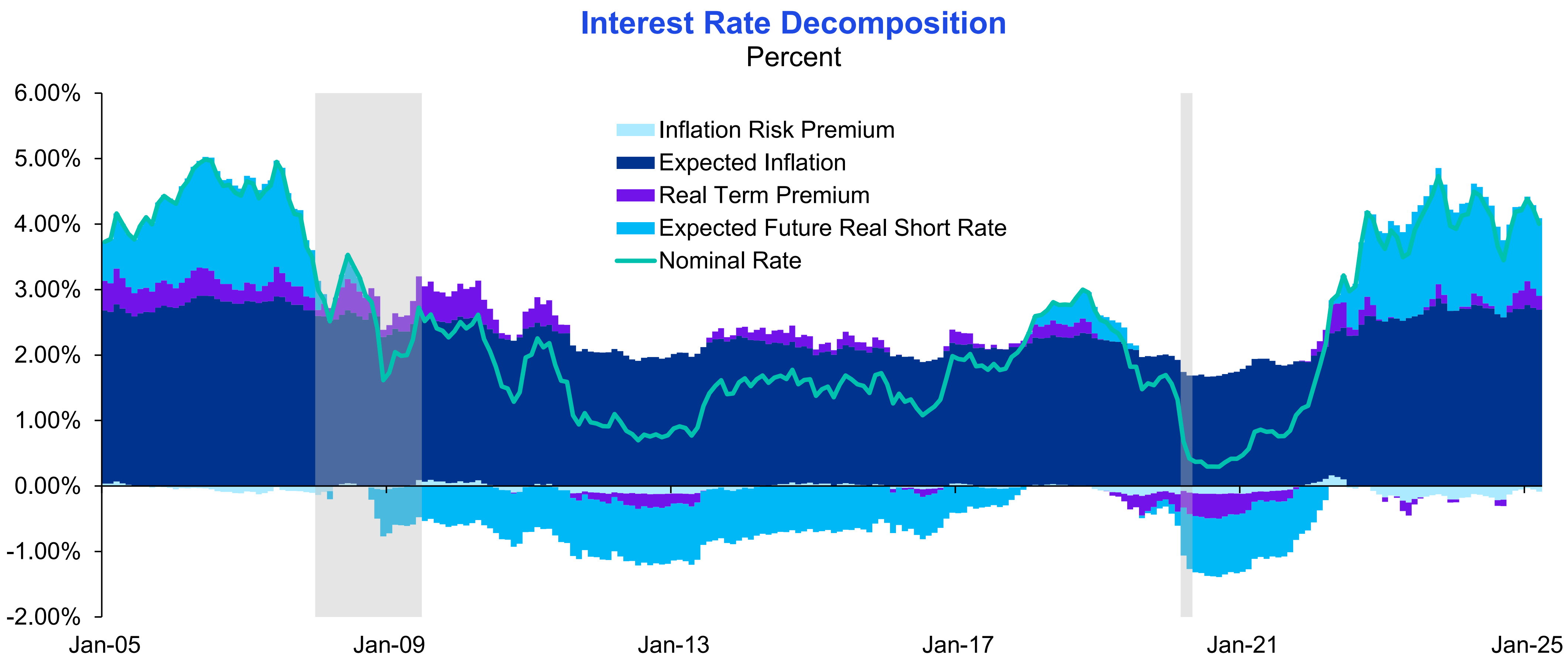
Source: KPMG Economics, KPMG Supply Chain, Federal Reserve Bank of New York

Aggregate prices increases in the past; tariffs to exacerbate



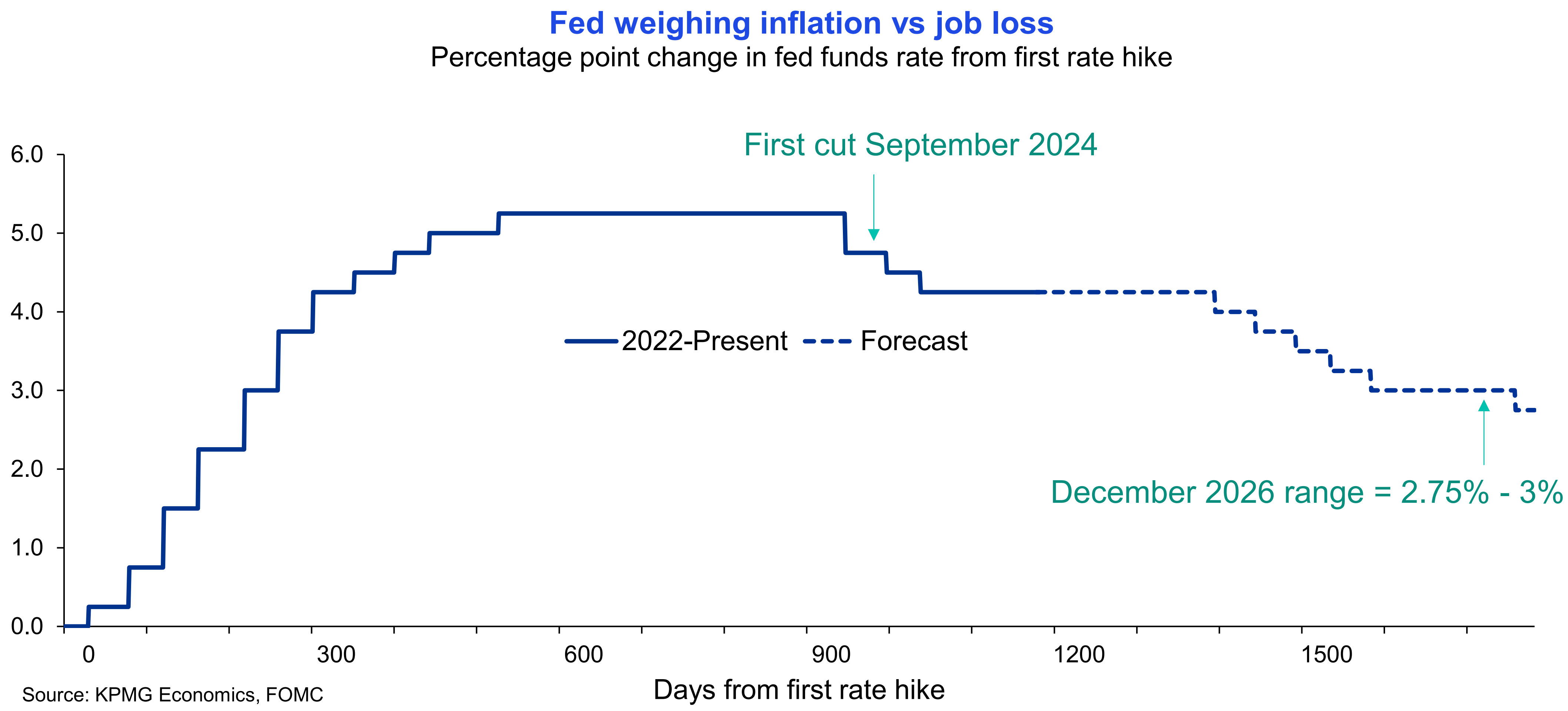
Source: KPMG Economics, Bureau of Economic Analysis, Haver Analytics

Rates are structurally higher than in the era of "free money"



Source: KPMG Economics, D'Amico, Kim and Wei Model, Haver Analytics

Fed to start cutting later this year

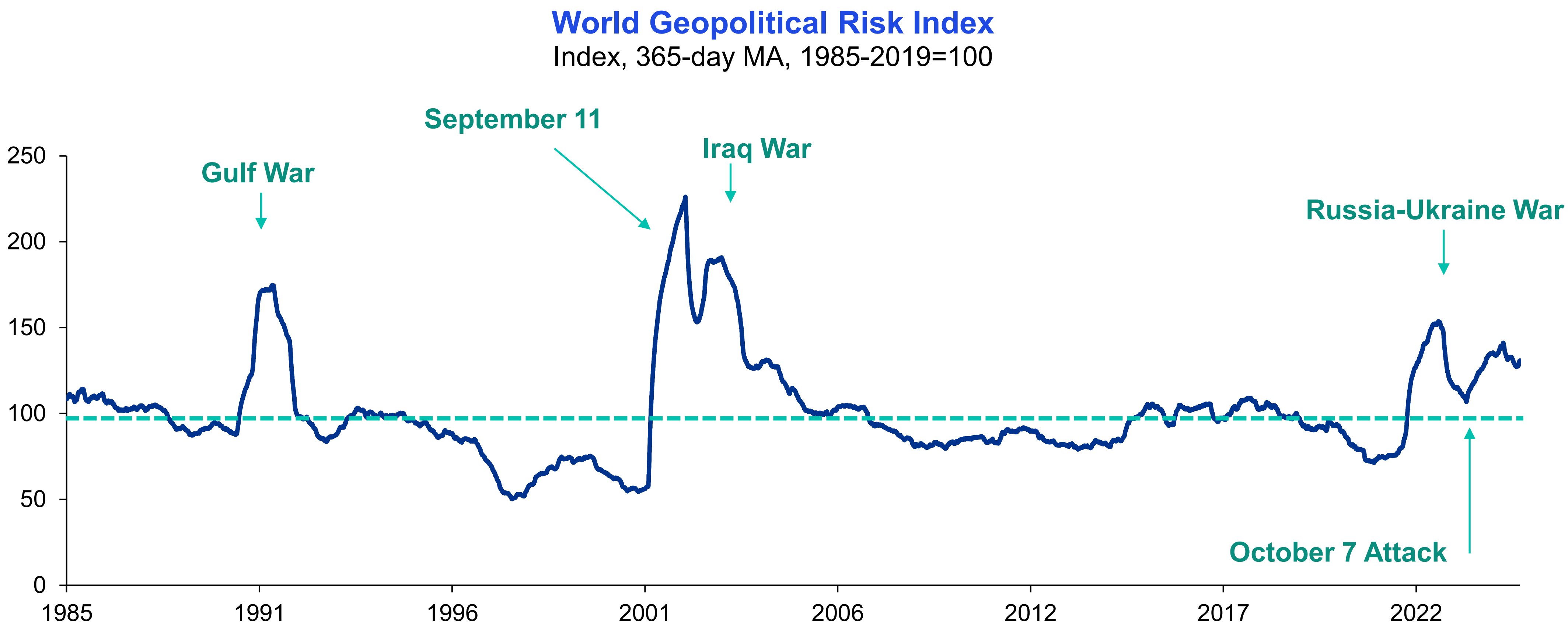


Source: KPMG Economics, FOMC

03

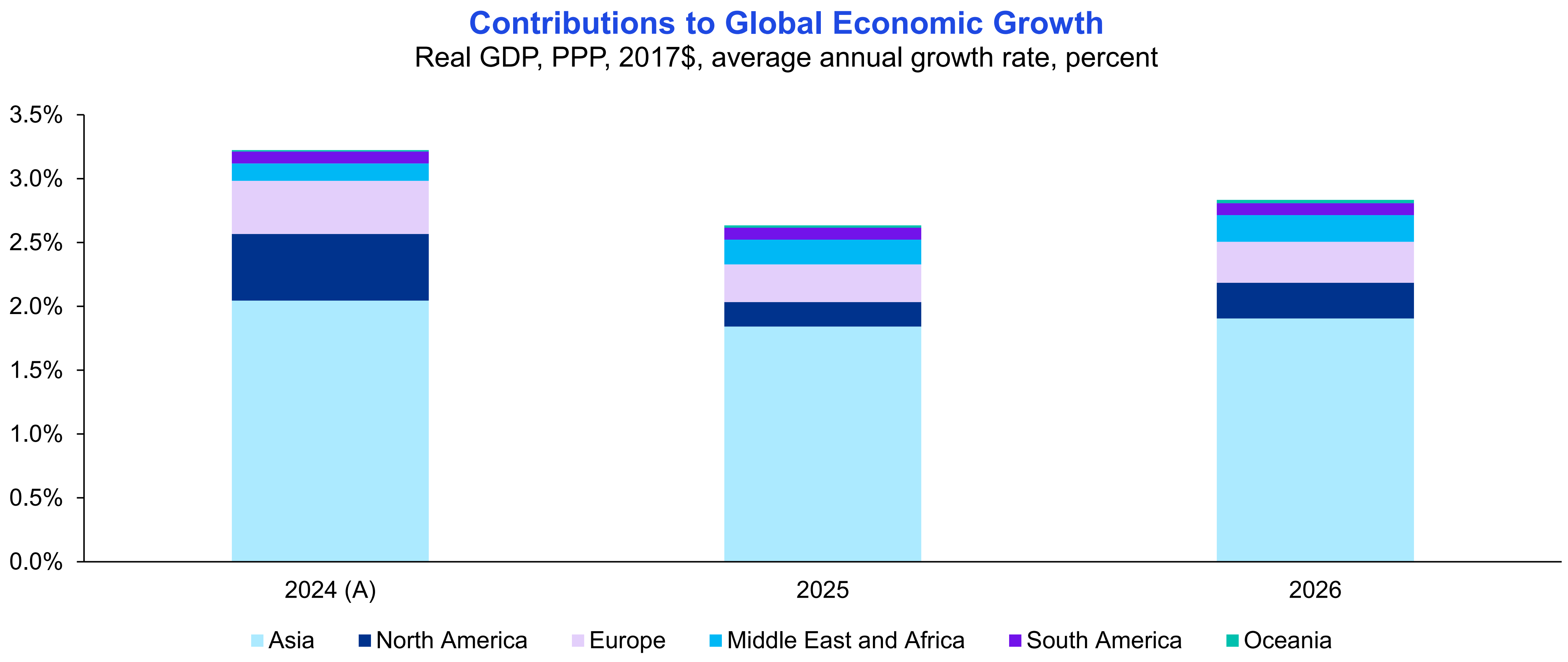
International Economy

Geopolitical risk remains elevated



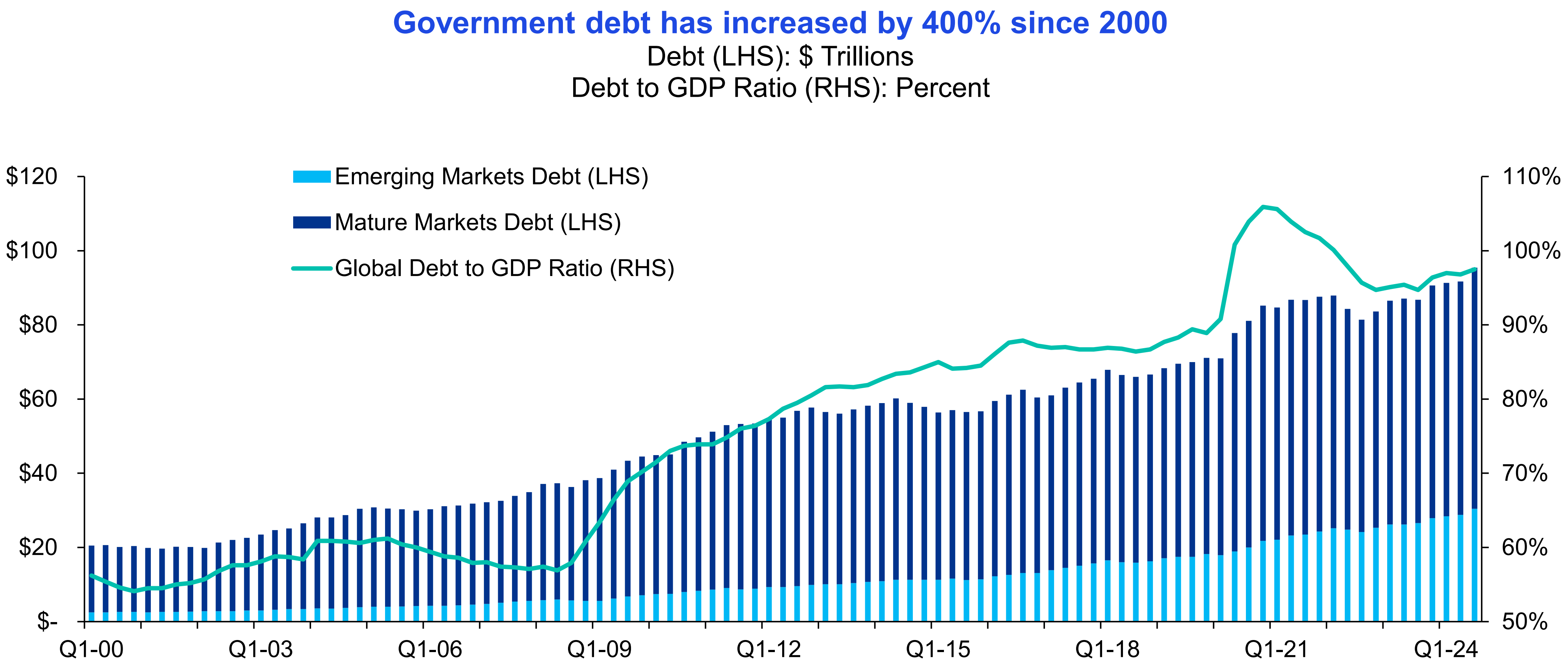
Source: KPMG Economics, Caldara and Iacoviello, Haver Analytics

Global growth to fall; avoids recession



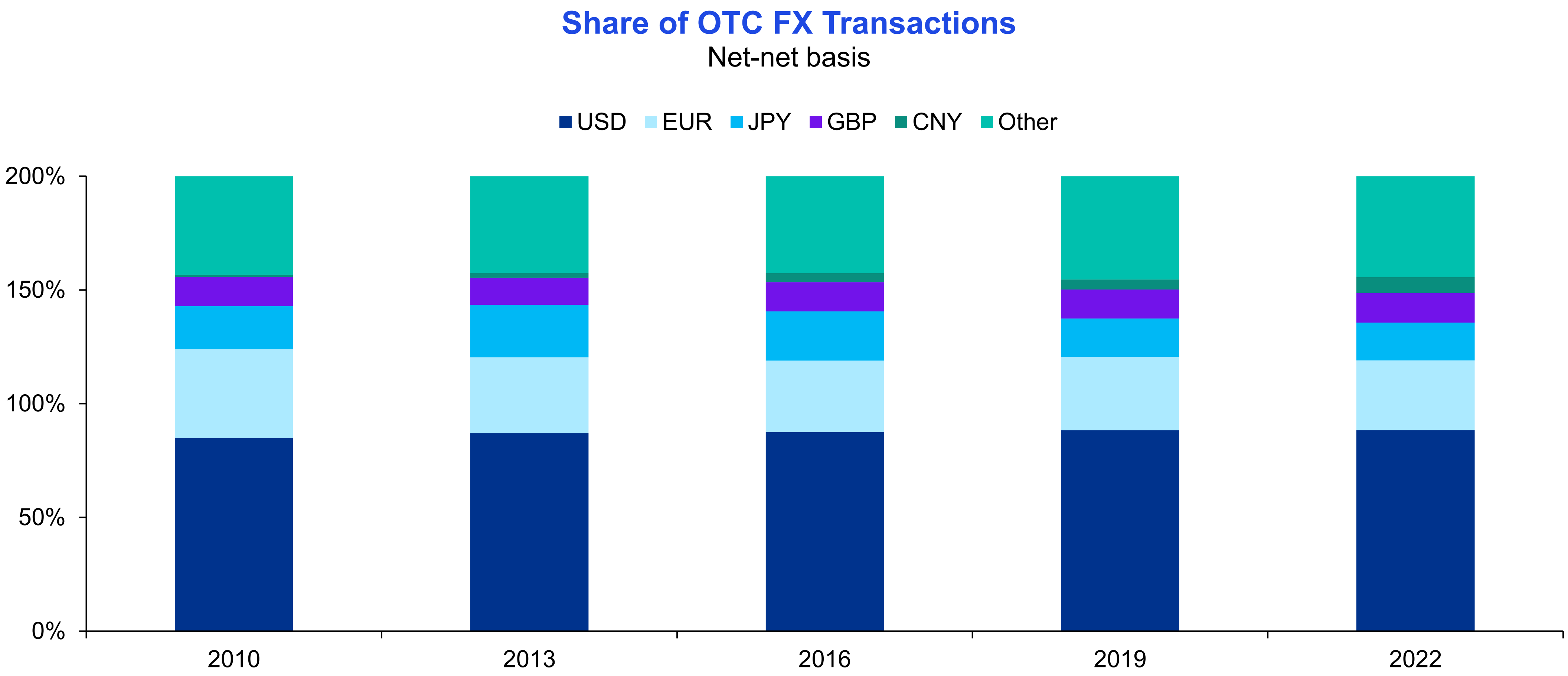
Source: KPMG Economics, Various

Stress on government coffers is mounting



Source: KPMG Economics, International Institute of Finance, Haver Analytics

The end of the dollar?

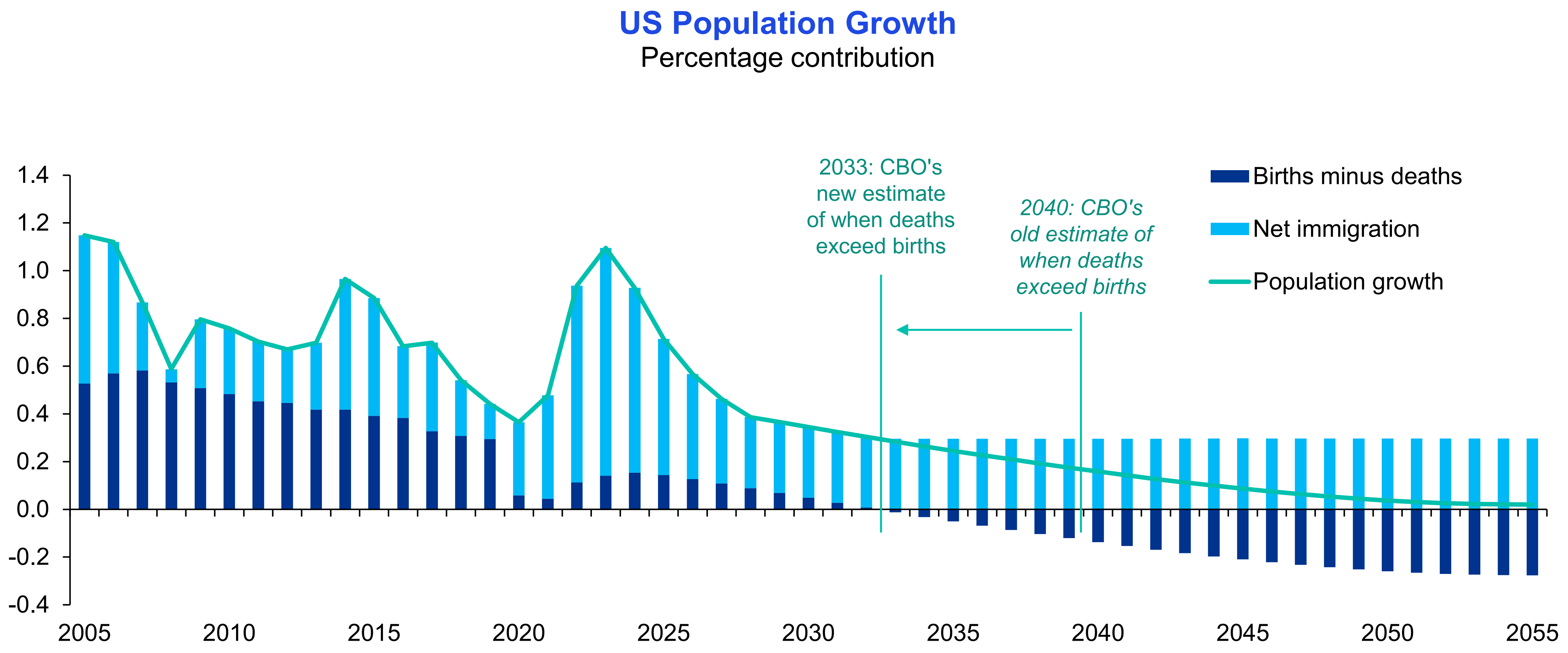


Source: KPMG Economics, Bank of International Settlements

04

Long-Term Trends

Immigration sole driver of US population growth in 20 years

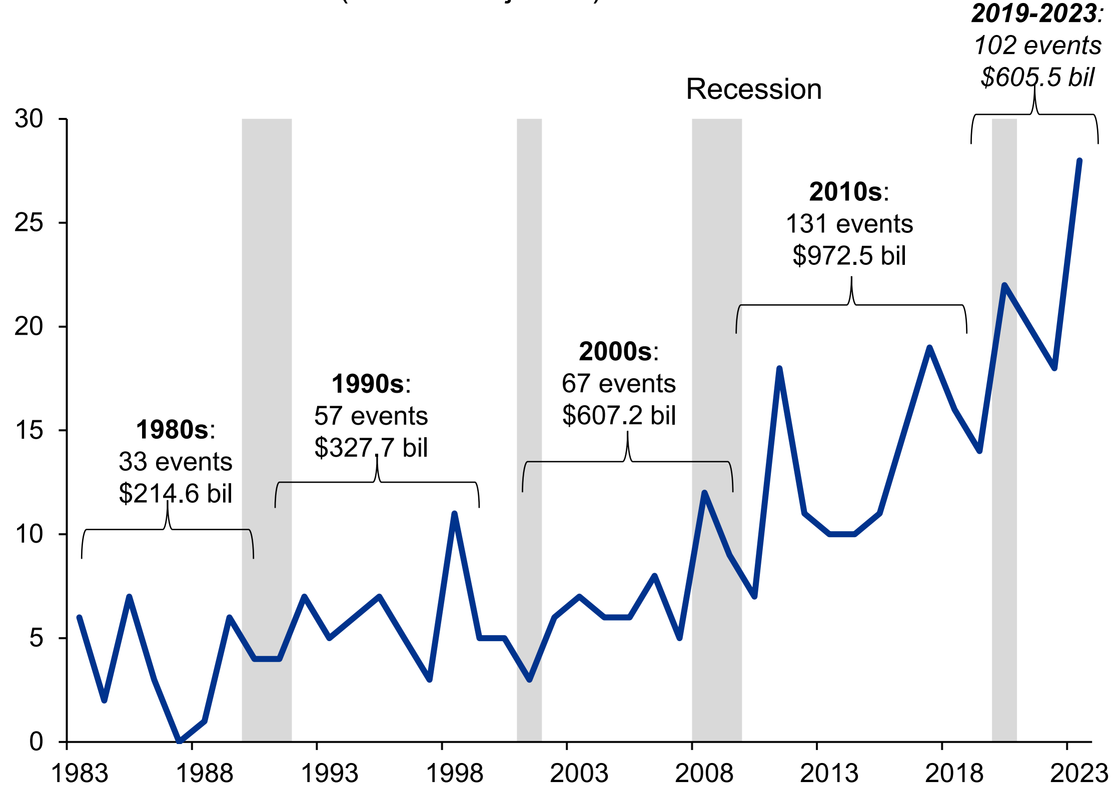


Source: Congressional Budget Office

Risks to supply chains are costly

Disasters getting more frequent

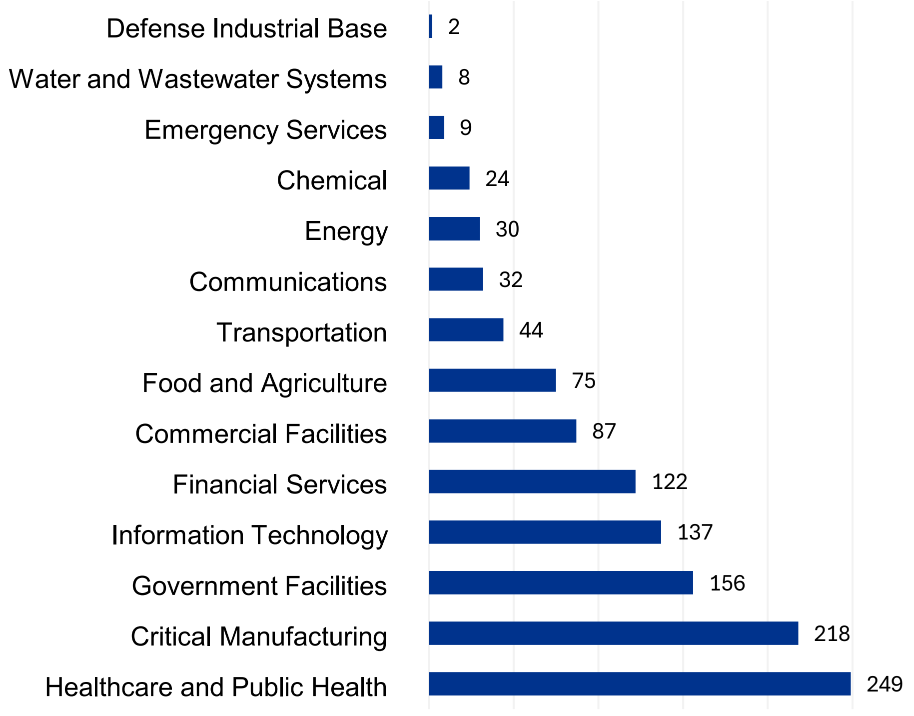
Number of (inflation-adjusted) billion dollar disasters



Source: KPMG Economics, NOAA

1,193 critical infrastructure companies affected by cyber strikes in 2023

Infrastructure Sectors Affected by Ransomware



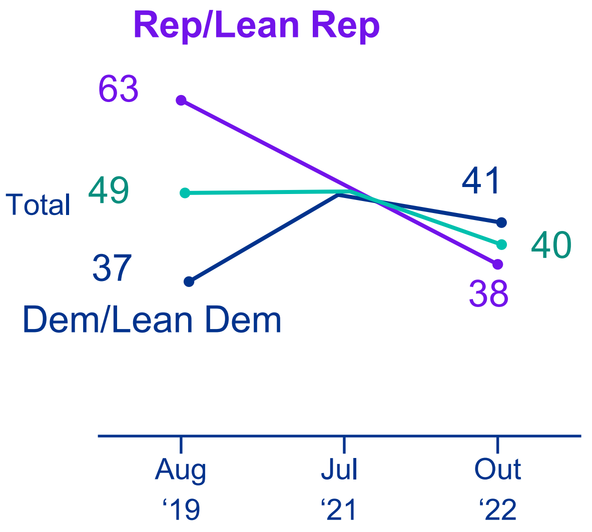
Source: FBI Internet Crime Complaint Center

Anti-corporate sentiment soars across party affiliation

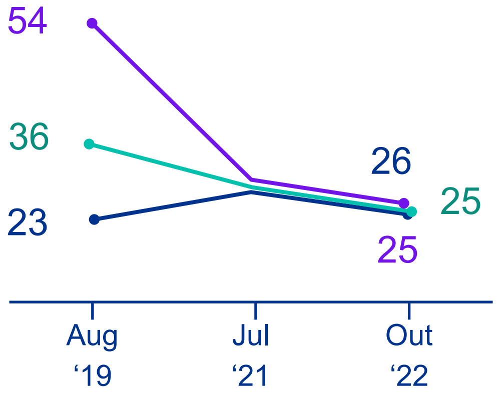
Republicans' views of banks, large corporations have become much less positive since 2019

% who say ____have a positive erect on the tray things are going in the country these days

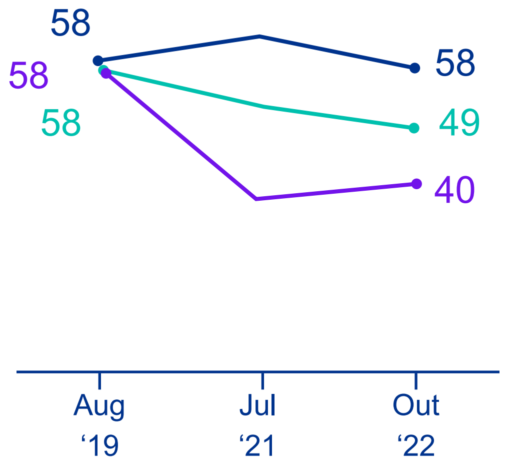
Banks and other financial institutions



Large corporations



Technology companies



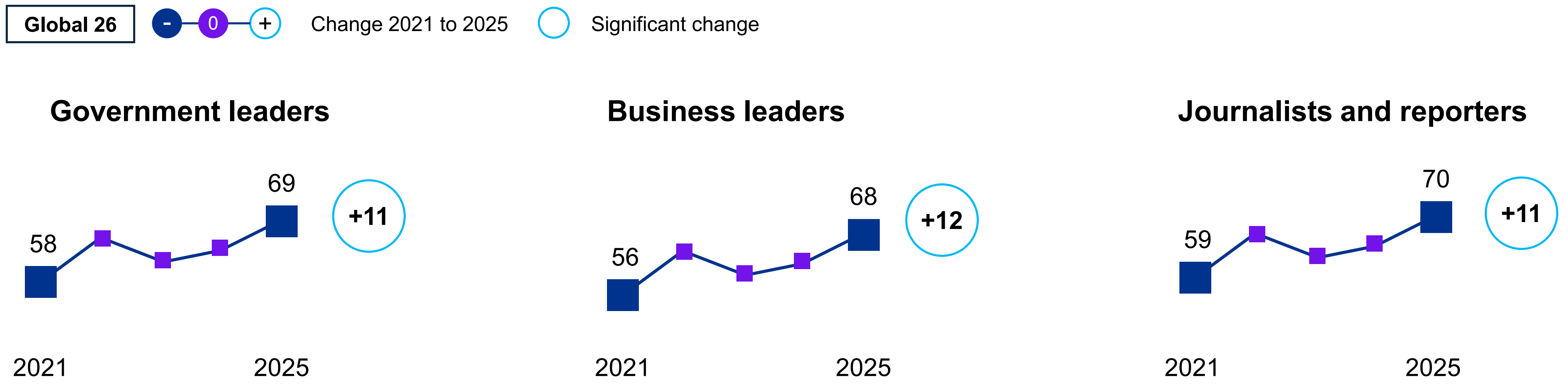
Source: Survey of U.S. adults conducted Oct. 10-16, 2022.

Pew Research center

Trust in leaders is eroding

Fear that leaders lie to us at All-Time High

Percent who worry



purposely mislead people

by saying things they know are false or gross exaggerations

2025 Edelman Trust Barometer. POP_EMO. Some people say they worry about many things while others say they have few concerns. We are interested in what you worry about. Specifically, how much do you worry about each of the following? 9-point scale; top4Box, worry. Attributes asked of half the sample. General population, 26-mkt avg. Year-over-year changes were tested for significance using a t-test set at the 99%+ confidence level. The all-time highs and lows analysis comprised countries with a least five waves of data collection.

For more KPMG Economics Insights, visit our website!

[KPMG Economic Insights]

Follow me on LinkedIn:

Ben Shoesmith
KPMG Senior Economist

Third Party Risk Management

Top Trends

Michael Bruner, Managing Director

Kyle Thompson, Director

June 26, 2025

TPRM Landscape

External factors

- Expanding ecosystems
- Geopolitical events
- Economic turbulence
- Emerging risks
- Regulatory focus
- Resourcing and skills

Third Party Risk Market Perspectives

72% Significant disruption, monetary loss or reputational damage

78% TPRM should be playing a more active role in Operational Resilience

63% TPRM is not yet a strategic partner to the business

Common Global Regulatory Themes

While globally different regulators have published their own regulations, there are a number of commonalities across these.

Resilience outcomes are at the heart of the regulations and these 6 key components help drive towards this outcome.

01 **Governance & accountability**
There is a clear expectation for Boards to be aware of and be involved in the decision making across the lifecycle of the most critical and material third party arrangements.

02 **Risk-based approach**
Identifying the most material and critical third-party arrangements and the highest risk domains in a given arrangement is key to a proportionate, risk-based approach.

03 **Due diligence**
Strengthening the due diligence performed on third parties and the contractual terms with material third party service providers

04 **Fourth parties and concentration risk**
The regulations go beyond third parties and require consideration of 4^{th} party suppliers. There is a need to assess concentration risk at both 3^{rd} and 4^{th} party level.

05 **Criticality of data and strong inventory**
A key element is having a comprehensive and accurate inventory of suppliers. Regulators are collecting industry data on material third party arrangements to assess systemic risks to the financial system.

06 **Contingency and exit planning**
Enhancing the resilience of third-party arrangements is essential. Regulators expect practical contingency and exit planning to deal with stressed events and potential exit of material third party arrangements.

07 **Contracting**
Comprehensive and up-to-date contracts to address assurance of rights and obligations, specific powers, and regulatory compliance.

02

TPRM – a deeper dive

TPRM Lifecyle

TPRM Relationships are managed at the legal entity level with the TPRM lifecycle set across five main phases, beginning with the planning and identification of potential third parties to their off-boarding or renewal. A relationship is one where a Company Division engages with an external third party to provide an activity that would otherwise be performed by the Company. The Residual Risk Rating (RRR) will drive various requirements, such as additional contractual provisions and ongoing monitoring activities.

Planning and Inherent Risk

A Relationship Owner (RO) should understand the needs of the Business and the risks that are exposed through the outsourced activity capturing these within the TPRM process.

Main processes:

- Identify business need for third party
- Complete IRQ
- Inherent risk rating is systemically calculated

Due Diligence/ Oversight Governance

The RO is responsible for ensuring that due diligence is completed and relevant risk summary reviews and approvals are completed/obtained prior to contract execution.

Main processes:

- Third party completes applicable Due Diligence and performs risk assessment mitigation activities as applicable
- Reviews Sign-Off Risk Summary

Contract Creation/ Onboarding

The RO accepts the contract terms while Procurement negotiates the contract terms in accordance with the assessed risk and existing control landscape.

Main processes:

<u>Prior to Contract Execution</u>

- Risk Reviews Completed
- Approvals are obtained from relevant/necessary Company stakeholders (i.e., Oversight Governance Committee (OCG))

Ongoing Monitoring (Contract/Risk Monitoring)

The RO is responsible to manage and oversee contract and service delivery. The RO must also manage the risks associated with the relationship.

Main processes:

- Track and monitor third party performance
- Track, report, remediate third party issues
- Manage onboarding/offboarding of contingent workers
- **Refresh**: The RO ensures IRQ is updated to reflect services (including material changes to services)

Termination

At the end of the lifecycle, services will terminated. **The RO responsibilities differ** depending on the path the relationship will follow.

Main processes:

- The RO is responsible to initiate relationship termination.
- The RO is responsible to execute exit plan/contingency plan
- Data consideration (Recovery etc.)

Holistic TPRM Operating Model

KPMG's TPRM services to assess, transform, and run TPRM programs are centered on our TPRM operating model below:

A TPRM framework built along three lines of defense (LOD) promotes agility, identifies emerging risks, and helps clarify an organization's strengths and weaknesses:

- 1st LOD: business process owners
- 2nd LOD: compliance oversight and centralized risk management functions
- 3rd LOD: independent assurance function or internal audit

Risk domains

Geopolitical/ country risk	Privacy risk	Fraud risk	Litigation risk
Regulatory/ Compliance risk	Subcontractor risk	Technology/ InfoSec risk	Financial viability
Strategic risk	Concentration risk	Reputational risk	Operational/supply chain risk

Lifecycle phases

Planning & third party identification → Due diligence & risk decision → Contract management & on-boarding → Ongoing monitoring → Off-boarding

Foundations of a TPRM program

- Policies and procedures
- Organization, people, skills, and training
- Governance and program effectiveness
- Data and reporting processes
- Enabling technology

The Value in Addressing TPRM Challenges

The insights below demonstrate the value from getting the balance between efficiency and effectiveness right.

People (Across 3LoD)

- Overclassified critical/high-rated third parties are driving increased cost of oversight by 35%.
- Centralized TPRM teams can reduce workloads of relationship owners by up to 80% and decrease risk team involvement by 40–60%.
- Use of specialty programs leads to quicker throughput time, approximately by 5–10 days.
- Employee resistance to change is a top-five reason TPRM programs don't realize full potential.

Process Pain Points

- Lack of integration between Procurement and TPRM around intake increases through put time by up to 40%.
- 30–60% of TPRM processes are manual, causing unnecessary operating and headcount costs.
- Revising risk and procurement questionnaires can lead to 30–50% reduction in overall question count.

Technology Integration

- A fully integrated TPRM architecture process can reduce operating costs by 20–35%.
- Central planning and intake can reduce error rates by 10–15%.
- A common TPRM language eliminates up to 25% of effort over the course of a year for a top-tier client across the lifecycle.

Risk Framework

- Right-size critical vendor list to <100 to allow for appropriate oversight.
- 50% of clients surveyed are planning to incorporate the "E" of ESG into TPRM in the coming 18–24 months.
- 80% of our clients are working on enhancing their fourth party risk management program oversight.

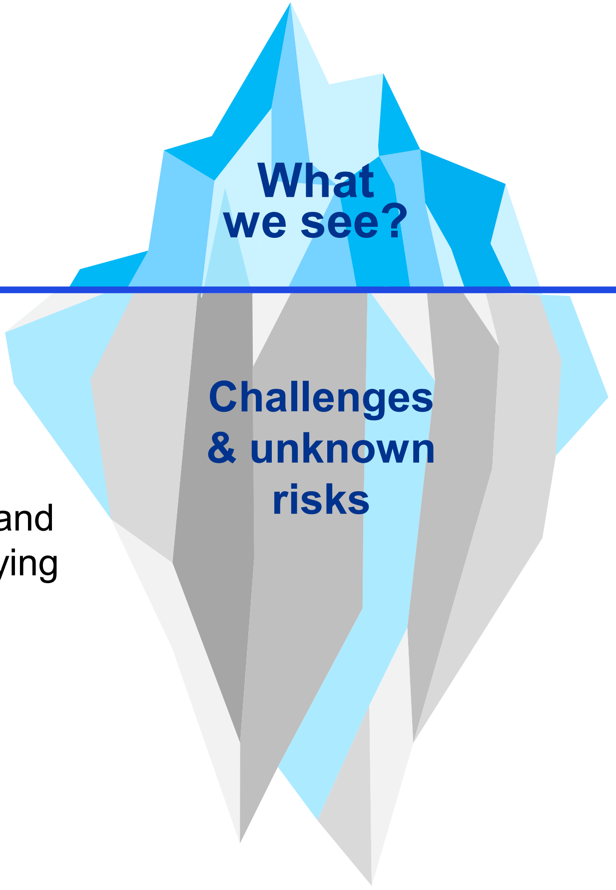
Data Reporting

- Leading institutions are building next-gen TPRM scoring methodologies using AI to speed up risk assessment process and better allocate TPRM resources, resulting in overall reduction of scoring effort by 30–50%.
- 40% of clients have suffered a disruption in BAU activities during the pandemic as a result of a third-party failure.
- Approximately 75% of our clients state that technology is the primary driver for the lack of clarity in TPRM reporting across procurement, risk and the business.

Fourth Parties and Sub-Contracting

Third parties have been the priority until recently – there is now a business, regulatory, and industry trend to widen the scope of TPRM oversight to fourth parties and beyond.

This is primarily driven by the resilience agenda and the extension of supply chains.



01

Supply Chains are increasingly complex, and challenges with identifying material suppliers is exacerbated by lack of data and effective process in place.

02

Ensuring the quality, relevance and timely reporting of fourth party data is difficult.

03

Complex supply chain can potentially lead to unmanageable amounts of data resulting in challenges identifying and prioritising the right information.

04

Fourth Parties are not governed by a contractual relationship with the organization, making prudent risk management of fourth parties challenging.

Concentration Risk

Concentration is a significant risk factor as it can lead to a single point of failure in the supply chain.

The risk arises when an organization relies heavily on a single third party or a small group of third parties for critical services.

Main types of concentration:

- Single supplier, multiple services
- Geographical concentration of suppliers
- Fourth party concentration across multiple services
- Lack of substitutability

Concentration Risk

Systemic Risk

Systemic Risk stems from industry-wide concentration of services with a single or limited set of third party(s) and is typically beyond the control of a single organization to manage.

Examples include:

- Telecommunications Providers
- Hyperscale Cloud Providers

Firm or Group-Wide Risk

Firm or Group-Wide Risk is the risk that an organization's operations or financial performance may be negatively impacted due to its reliance on a limited number of suppliers. It can arise when:

- **Third Party Diversity –** A single supplier or a small group of suppliers provides a significant portion of the organization's needs for a particular item.
- **Substitutability –** The organization has limited alternative sources of supply for the item.
- **Criticality –** The service is critical to the organization's operations or financial performance.

Continuous Monitoring and Reporting

Historic approaches to risk assessments, monitoring and reporting have inherent limitations.

Point-in-time assessments have a strong role to play, however their effectiveness is limited.

Continuous Monitoring & Reporting Challenges

01

TPRM reporting is slow and manual

- Traditional TPRM reporting systems are often manual and slow, leading to delays in accessing real-time data.

02

Data access & availability

- Obtaining timely, accurate data from third party providers is often challenging.
- Cycle times are elongated and risk reports are often out of date by the time they are published.

03

Scalability

- As the number of third and fourth parties grows, scaling up the approach and operating model is key.

04

Data quality

- Inconsistent data sources and reporting standards can result in unreliable risk indicators.

05

Resource constraints

- Many companies are subject to investment restrictions and headcount freezes are in place. This is limiting the amount of monitoring that can be performed.

Continuous Monitoring & Reporting

Many companies are prioritizing continuous monitoring in addition to point-in-time risk assessments.

This is a way to identify early warning indicators for potential third party outages or an increase in the risk profile of the third party service.

Continuous monitoring is dependent on leveraging data and technology.

The adoption and maturing of AI will help drive up the amount of continuous monitoring that can be done.

Components of Continuous Monitoring

1. **Performance Assessment** Business owner third party performance assessment, via scorecards
2. **SLA Monitoring** SLA monitoring via contract management tools
3. **Financial Monitoring** Including fraud and financial health
4. **Risk Data** Including adverse media, cyber breaches, assurance reports, financial crime, ESG, etc.

High-quality data & fit-for-purpose tooling

- Financial Oversight
- Contract Management
- Risk Intelligence
- Program Oversight
- Ongoing Monitoring

Data Lake (transforms Data)

AI Risk in Third Parties

Many companies are adopting AI. There is a lack of visibility over the changes and transformation occurring in the third parties and their supply chain.

The criticality of the changes and their impact on important and critical business services is not well understood or managed at present.

Third Party AI Risk Challenges

01 Third and Fourth Parties are already using AI

02 There is often a lack of visibility of AI use in the supply chain

03 It is often unclear what impact use of AI has or could have on services and value streams

04 Contractual coverage may not encompass AI

05 AI-specific policies and standards may not be in place for third parties to follow

06 It is often unknown how business data and customer data is being used within 3rd party AI models

07 **Ensuring compliance with evolving global regulations**

Managing AI Risk in Third Parties

For both new and existing third-party arrangements, there is a need to identify where AI is used, undertake an assessment of the risk to companies and remediate as required.

Ensure AI risk is a key component of the third-party due diligence and contracting process.

New

01 Discovery

Conduct a risk assessment of new and existing third parties to identify use of AI by the third party.

Do you have visibility of the AI use by your critical third parties?

02 Inventory

Compile an inventory of AI models in the third party, including data utilised.

Do you have visibility of the AI model inventory?

03 Critical Services

Understand and register AI use across your organization, evaluating risks, controls and capabilities, security, privacy practices etc.

Have you assessed criticality, risk and controls across your third-party landscape?

04 Contracting

Review existing contracts and update contractual terms in line with Board AI risk appetite.

Set process for new contracts.

Have contracts, policies and procedures been reviewed and updated to reflect AI?

05 Monitoring

Monitor the performance of third party's AI models to ensure that they are functioning as expected and are operating in a controlled way.

What additional monitoring do you need to implement?

Existing Contracts

What does the future of TPRM look like?

Proportionate and risk-based framework

- Assesses the control environment and risk profile of third-party services in a risk proportionate way
- Materiality and inherent risk drives scope and focus of TPRM activity through tiering
- Focused on achieving risk reduction and resilience outcomes

Consistent across the enterprise

- TPRM activities across the organization are joined up and consistent; not siloed
- Language, methodology and reporting are aligned across divisions, regions and risk domains
- Risk domain and other SMEs are integrated into the processes; aligned with 1LoD teams, and across 2LoD & 3LoD

Compliant and efficient

- Policy and regulatory expectations are met
- Onboarding and cycle times are optimized
- Processes are streamlined and simple/easy to navigate; user experience is positive
- Technology automates workflow tasks
- Costs commensurate with value outcomes

Integrated with complementary processes and tools

- TPRM processes integrate with procurement, contracting and issue/risk management
- TPRM outcomes feed into sourcing & contracting decision-making
- Internal and external data sources inform tiering and enable focus on areas of highest risk
- Data drives 4th party and concentration risk analysis

Enablers

Leadership and governance – Prominent function, with strong leadership; full business-wide buy-in

Data-driven – Intelligence built-in to tiering and assessment framework; quality data drives inventory, risk metrics, and reporting

Automation – Standardized and easy to use processes; portals for third party data exchange, live monitoring, and AI-enabled

Resources – Sufficient and appropriately skilled capability, able to scale if required; low-cost locations/delivery model

Operating model – Well defined RACI; fully joined up model across all teams and LoDs

June 2025
Chapter Meeting

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**