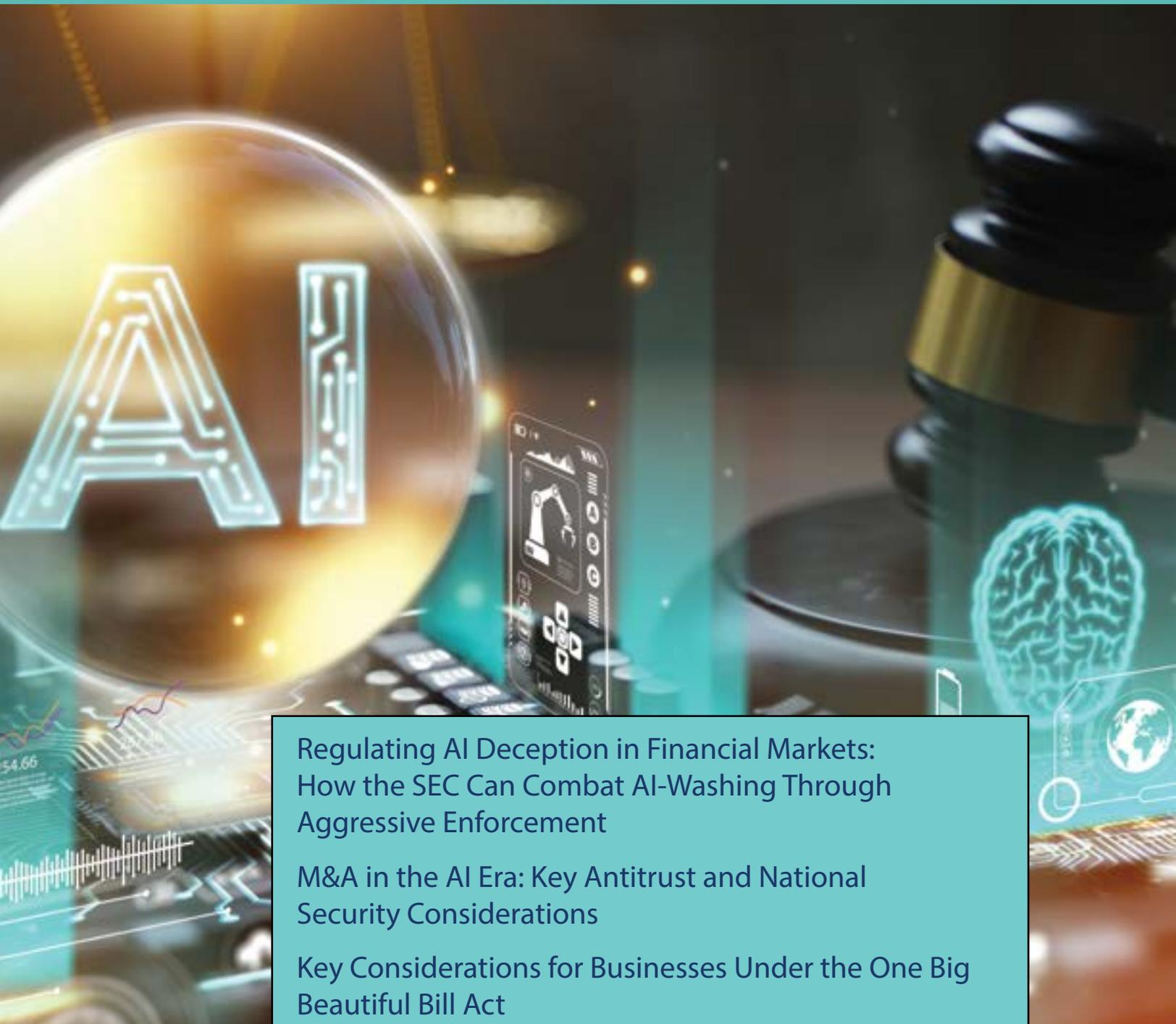




2025 | VOL. 29 | NO. 2

# NY Business Law Journal

A publication of the Business Law Section of the New York State Bar Association



Regulating AI Deception in Financial Markets:  
How the SEC Can Combat AI-Washing Through  
Aggressive Enforcement

M&A in the AI Era: Key Antitrust and National  
Security Considerations

Key Considerations for Businesses Under the One Big  
Beautiful Bill Act

# M&A in the AI Era: Key Antitrust and National Security Considerations

By Christopher M. Barlow, Ken D. Kumayama, Sonia K. Nijjar, Katie Clarke and Yingchuan (Grace) Mo



## Key Points

- As more jurisdictions adopt AI regulations, and AI-related transactions are reviewed on multiple legal grounds, it is critical for companies considering deals to assess the regulatory hurdles early on and develop a strategy to mitigate risks and maximize deal certainty.
- Beyond AI regulations generally, M&A transactions involving AI may be subject to increasing scrutiny under antitrust and national security laws.
- Alternative deal structures that can address regulators' concerns in some cases include minority investments without control rights, contractual limitations on data access and carve-outs of sensitive technologies or entities.

As artificial intelligence (AI) continues to drive innovation and competitiveness across industries, acquiring businesses with a significant AI component has become a key piece of many companies' overall strategy. However, these transactions bring with them a distinct set of complexities, shaped

by a rapidly evolving technological landscape and an increasingly complex regulatory environment.

## Proliferating Regulatory Regimes

AI is subject to an ever-growing number of regulatory regimes. For example, in the European Union, the AI Act – which applies broadly to providers, deployers, importers and distributors of AI systems – went into effect on August 1, 2024, and will become fully enforceable on August 2, 2027.

In the U.S., the Trump administration revoked the prior administration's "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" executive order, replacing it with a new executive order titled "Removing Barriers to American Leadership in Artificial Intelligence," issued on January 23, 2025.

The new order directed certain federal agencies to develop a coordinated action plan within 180 days to sustain and enhance America's global AI dominance. Relatedly, on April 3, 2025, the Trump administration issued two memo-

randa outlining how federal agencies should use and procure AI technologies.

Meanwhile, at the state level, Utah, Colorado and, most recently, Texas, among others, have enacted AI-specific laws regulating the development, deployment and disclosure of AI tools. Alongside these AI-specific requirements, existing federal, state and international data privacy laws continue to govern the collection and use of personal data in training AI models, adding yet another layer of compliance complexity.

In light of these regulatory developments and the unique risks and opportunities AI technologies present, M&A deal terms have been – and will continue to be – adapted to allocate and manage potential AI-related liability exposure between the transacting parties.<sup>1</sup>

Beyond AI regulations generally, two regimes are particularly consequential in the context of M&A transactions: antitrust and national security.

Regulators in the U.S. and abroad have shown growing interest in M&A transactions involving AI companies, recognizing the sector’s strategic importance and the potential competitive implications of consolidation. Parties contemplating such deals should engage counsel with deep expertise in both antitrust and national security laws to proactively assess risks, optimize deal structures and position the transaction to obtain regulatory clearance.

## Antitrust Considerations

Antitrust regulators are increasingly wary of Big Tech’s market dominance, particularly as these companies acquire or partner with AI startups that may one day challenge Big Tech companies’ positions. Concerned about consolidation in a nascent but strategically critical sector, competition authorities are paying closer attention to how deals are structured – even when they fall below traditional reporting thresholds.

Big Tech companies have become top acquirers of AI startups in recent years. Although their acquisitions might not be inherently anticompetitive, they frequently attract heightened attention from regulators, reflecting concerns that small acquisitions today may preempt significant competition tomorrow. This proactive stance underscores regulators’ intent to prevent the incumbents from entrenching market dominance by absorbing potential future competitors.

In response, some Big Tech companies have employed alternative structures, such as “acquihires” – hiring key talent and acquiring or licensing core intellectual property rather than buying the entire business. However, acquihires increasingly face regulatory scrutiny, as illustrated by investigations conducted by the U.K. Competition and Markets Authority (CMA), German Federal Cartel Office (FCO) and U.S. Fed-

“U.S. policymakers are increasingly focused on both inbound and outbound investments involving AI technologies, as well as the potential transfer of sensitive data to foreign adversaries. This has led to a wave of new regulatory measures designed to safeguard U.S. technological leadership and national security interests.”

eral Trade Commission (FTC) into the acquire transaction between Microsoft and Inflection AI.

Although both the CMA and FCO ultimately closed their inquiries due to Inflection AI’s limited market presence, the FTC’s investigation continues, and its outcome may shape how acquihires are treated under U.S. merger review standards going forward.

Strategic partnerships, involving equity investments and technical collaboration without full acquisition, have also emerged as a common alternative. These arrangements offer flexibility and speed but may attract regulatory attention as potential “backdoor acquisitions” – particularly when they involve governance rights (e.g., board seats or observer roles), preferential access to AI technologies or exclusivity.

Recent regulatory reviews – including the CMA’s investigation into Microsoft’s partnership with OpenAI and the FTC’s examination of partnerships between major cloud providers (Alphabet, Amazon, Microsoft) and leading generative AI developers (Anthropic, OpenAI) – highlight the regulatory sensitivity surrounding nontraditional deal structures in the AI space. While the CMA ultimately closed its review after Microsoft relinquished its OpenAI board observer seat, it remains to be seen how the FTC under new Chairman Andrew Ferguson’s leadership will view the impact of these partnerships on competition.

As antitrust scrutiny of AI transactions intensifies, parties should consider preparing for increased oversight (even where no formal change of control occurs), working closely with antitrust counsel to assess risk early in the process, and adopting structural or behavioral measures that may help mitigate antitrust concerns.

## National Security Considerations

Growing national security concerns have placed cross-border transactions in the AI sector under heightened scrutiny as well. U.S. policymakers are increasingly focused on both inbound and outbound investments involving AI technologies, as well as the potential transfer of sensitive data to foreign adversaries. This has led to a wave of new regulatory measures designed to safeguard U.S. technological leadership and national security interests.

### Reverse CFIUS

On January 2, 2025, the Department of the Treasury's "reverse CFIUS" outbound investment security program went into effect, establishing a new investment screening framework for investment in China by U.S. persons. The regime imposes due diligence obligations, record-keeping and notification requirements, and restrictions on U.S. persons and their controlled foreign entities engaging in M&A or other covered transactions with foreign persons in "countries of concern" (currently limited to China) that perform defined activities related to AI and other sensitive technologies.

### America First Investment Policy

On February 21, 2025, the White House released President Donald Trump's "America First Investment Policy" memorandum. This national security policy memo signals a potential expansion of both inbound and outbound investment restrictions to address national security risks posed by Chinese involvement in AI and other emerging technologies, while making clear that the Trump administration will still welcome foreign investment from allies and partners in these key sectors. On May 8, 2025, the Treasury Department announced that, consistent with the America First Investment Policy, it will conduct a pilot fast-track process, including the launch of a Known Investor portal, to streamline the Committee on Foreign Investment in the United States' (CFIUS) reviews and facilitate greater investment in U.S. businesses from allied and partner nations.

### DOJ Restrictions on Certain Investments

On April 8, 2025, the Department of Justice (DOJ) implemented a final rule, restricting or prohibiting certain investments and business arrangements involving U.S. sensitive personal data or government-related data with foreign persons in China, Russia and other designated jurisdictions. The rule reflects concerns that the advancement of AI and other emerging technologies in these countries amplifies the national security risks associated with their potential access to such data.

In addition to these U.S. regulatory regimes, parties weighing cross-border transactions must consider whether an investment may trigger foreign direct investment reviews in

other jurisdictions. While the breadth of these regimes vary greatly, under many of them, the involvement of AI technology triggers filing requirements.

Such regimes have proliferated in the last five years and, without a coordinated strategy across jurisdictions early in the process, parties can face increased transaction costs and timing uncertainty.

In general, parties pursuing cross-border transactions involving AI technologies should anticipate greater compliance obligations, more extensive diligence requirements and longer regulatory review timelines.

Early stage national security risk assessments are critical to determine whether a proposed deal may trigger U.S. or foreign national security review (or be prohibited under the "reverse CFIUS" program). To navigate this evolving landscape, parties may also want to consider structuring alternatives, such as:

- Minority investments without control rights.
- Contractual limitations on data access.
- Transaction structures that carve out sensitive technologies or entities.

These approaches may help mitigate regulatory risk and preserve deal certainty in an increasingly complex geopolitical environment.

The authors are attorneys at Skadden, Arps, Slate, Meagher & Flom LLP. **Christopher M. Barlow** is a partner in mergers & acquisitions in New York. **Ken D. Kumayama** is a partner in intellectual property and technology and privacy in Palo Alto. **Sonia K. Nijjar** is a partner in mergers and acquisitions in Palo Alto. **Katie Clarke** is counsel on cross-border and national security, primarily involving reviews by the CFIUS, in Washington, D.C. **Yingchuan (Grace) Mo** is corporate counsel in Palo Alto.

### Endnote

1. For a discussion of such deal terms, see our June 2024 article *M&A in the AI Era: Key Deal Terms To Watch*, Skadden.com, <https://www.skadden.com/insights/publications/2024/06/quarterly-insights/ma-in-the-ai-era-key-deal-terms-to-watch>.