Unterberg, Bovenzi, Sinai and Garcia in Law360 Banking Brief: All The Notable Legal Updates In Q4

January 8, 2025 Craig Unterberg, Giorgio Bovenzi, Krista Garcia

PRACTICES Finance, Financial Regulatory

Haynes Boone attorneys Craig Unterberg, Giorgio Bovenzi, Leel Sinai, Krista Garcia and law clerk Livingstone Harriott contributed to the fourth quarter edition of the NY Banking Brief from *Law360*, discussing the biggest developments in New York banking regulation and policymaking.

Read an excerpt below.

In this fourth quarter edition of the NY Banking Brief, we summarize two pieces of guidance released by the New York State Department of Financial Services. The first concerns cybersecurity risks arising from the use of artificial intelligence, along with strategies to combat those risks, and the second covers threats posed by remote technology workers with ties to North Korea.

In addition, we discuss developments in New York's antitrust investigation of the proposed merger between Capital One and Discover Financial Services.

NYDFS Guidance on AI Cybersecurity Risks and Strategies to Combat Them
On Oct. 16, the NYDFS issued guidance to explain how to use the existing cybersecurity framework under Title 23 of the New York Codes, Rules and Regulations, Part 500, to address cybersecurity risks related to AI.[1]

Recent advancements in AI have significantly affected the cybersecurity landscape, both enhancing protection capabilities and creating new risks. For covered entities regulated by the NYDFS, AI has bolstered capabilities in preventing cyberattacks, improving threat detection and strengthening incident response. At the same time, AI has also introduced new exploitation opportunities, necessitating updated guidance to help covered entities understand and mitigate these risks.

Notably, this AI guidance does not introduce new requirements beyond those in Part 500.

The AI guidance's purpose is to highlight the impact of the recent AI developments on cybersecurity risk — and thus, the attention that all organizations should give while developing a cybersecurity program and implementing cybersecurity controls — and on the integration of AI into cybersecurity tools, controls and strategies.

The AI guidance ultimately urges covered entities to review and reevaluate their cybersecurity programs and controls at regular intervals — yearly, at a minimum — in compliance with the already existing parameters of the NYSDFS cybersecurity framework.

Risks Associated With AI
AI-related cybersecurity risks fall into two main categories: risks arising from threat actors using AI and risks stemming from a covered entity's reliance on AI.

Pointing out that "AI-enabled social engineering presents one of the most significant threats to the financial services sector," the AI guidance explains how AI has improved the sophistication of social

engineering attacks, making them more convincing and personalized.

Bad actors now use AI to create realistic deepfakes in audio, video and text formats, which can be used to lure targeted individuals into sharing sensitive information or performing unauthorized actions. This can lead to unauthorized access of nonpublic information, or NPI, as well as fraudulent wire transfers and the successful bypassing of biometric authentications.

The AI guidance also notes that AI accelerates the scale and speed of cyberattacks by allowing bad actors to rapidly identify and exploit vulnerabilities. AI can generate new malware variants and circumvent security controls, raising the volume and impact of attacks while lowering the barriers to entry for less skilled cybercriminals.

The AI guidance points out that an increase in the number and severity of cyberattacks can be expected in light of these factors. It also identifies the presence within the financial services sector of highly sensitive NPI that can be a lucrative target for criminals.

The AI guidance further notes that AI systems collect and process vast amounts of data, including NPI, giving bad actors the incentive to steal NPI — particularly biometric data — for financial gain or malicious use.

The AI guidance notes that AI systems rely on data from vendors and third-party service providers, or TPSPs, and such supply chain dependency introduces potential security vulnerabilities when the data is collected and gathered. Compromised vendors and TPSPs can expose the covered entity's NPI and become gateways for broader attacks.

To read the full article on *Law360*, click here.