INSIGHT

New York: NYDFS issues guidance on AI cybersecurity risks

6 days ago

Summary

The New York Department of Financial Services (NYDFS) issued guidance on October 16, 2024, for entities under its jurisdiction to assess and mitigate AI-related cybersecurity risks, without imposing new requirements but clarifying that AI risks should be considered under existing cybersecurity regulations. The guidance outlines specific AI-related threats, such as AI-enabled social engineering and AI-enhanced cyberattacks, and recommends controls and measures for mitigating these threats, including risk assessments, third-party management, access controls, cybersecurity training, and data management. It also discusses the broader implications of AI use in financial services and notes the trend of regulatory scrutiny and enforcement, highlighting actions by other states and federal agencies to manage AI risks in the financial sector.

NYDFS issues guidance on AI cybersecurity risks, outlining threats and mitigation strategies.

On October 16, 2024, the New York Department of Financial Services (NYDFS) issued an industry letter providing guidance on assessing and mitigating cybersecurity risks arising from the use of artificial intelligence (AI) (the Guidance), emphasizing the significant impact AI has had on

cybersecurity. Caleb Skeath, Micaela R.H. McMurrough, and Vanessa Lauber, from Covington & Burling LLP, explore the Guidance and how entities can assess and mitigate risks.

The Guidance applies to entities under the NYDFS jurisdiction, i.e., entities required to operate under a license or similar authorization by the New York Banking Law, the Insurance Law, or the Financial Services Law (collectively, Covered Entities). According to the NYDFS, the Guidance 'does not impose any new requirements' beyond those already present in NYDFS's landmark cybersecurity regulations, codified at 23 NYCRR §500 (the Cybersecurity Regulation), but rather sets forth good AI governance practices and clarifies how Covered Entities should address AI-related risks as part of the Cybersecurity Regulation. The Cybersecurity Regulation, as revised in November 2023, requires Covered Entities to implement certain detailed cybersecurity controls, including governance and board oversight requirements, as well as a risk-based cybersecurity program that meets certain requirements. Those cybersecurity controls must now account for AI-based cybersecurity risks as well.

The Guidance is notable for a few reasons. First, the need to address AI-related cyber risk applies across industries. For that reason, even companies that are not Covered Entities under the Cybersecurity Regulation may want to consider the Guidance if they are using or planning to use AI tools or capabilities, or if they could be vulnerable to any of the AI-related risks or attacks described below (and given the current landscape, it is difficult to think of many companies who would not fall into these categories). Entities across industry sectors that are required to adopt reasonable, risk-based cybersecurity programs can use the Guidance as input for how to address evolving AI-related risks. Second, as noted, the Guidance does not add any AI-specific requirements or revise the Cybersecurity Regulation in any way; it simply makes clear that Covered Entities should be considering AI risk as part of their reasonable cybersecurity program. In other words, the regulator is indicating that a requirement to manage AI-related risk is already baked into existing standards and signaling that it may police AI risk pursuant to existing authorities.

AI-related risks

AI has the potential to scale and amplify existent patterns of cyber risk, both as a source of external threat and in connection with internal use. The Guidance notes that threat actors have a 'lower barrier to entry' to conduct cyberattacks as a result of AI and identifies four specific (non-exhaustive) cybersecurity risks related to the use of AI, including two risks related to the use of AI by threat actors against Covered Entities.

- **AI-enabled social engineering** - The Guidance highlights that 'AI-enabled social engineering presents one of the most significant threats to the financial services sector.' For example, the Guidance observes that 'threat actors are increasingly using AI to create realistic and interactive audio, video, and text ('deepfakes') that allow them to target specific individuals via email (phishing), telephone (vishing), text (SMiShing), videoconferencing, and online postings.' AI-generated audio, video, and text can be used to target individuals to convince employees to divulge sensitive information about themselves or their employer, wire funds to fraudulent accounts, or circumvent biometric verification technology.
- **AI-enhanced cybersecurity attacks** - The Guidance notes that AI can be used by threat actors to amplify the potency, scale, and speed of existing types of cyberattacks by quickly and efficiently identifying and exploiting security vulnerabilities.

The Guidance also identifies two risks related to the use of or reliance on AI by Covered Entities.

- **Risks related to vast amounts of non-public information** - Covered Entities might maintain large quantities of non-public information, including biometric data, in connection with their deployment or use of AI. The Guidance notes that 'maintaining non-public information in large quantities poses additional risks for Covered Entities that develop or deploy AI because they need to protect substantially more data, and threat actors have a greater incentive to target these entities in an attempt to extract non-public information for financial gain or other malicious purposes.'

- **Vulnerabilities due to third-party, vendor, and other supply chain dependencies** - Finally, the Guidance flags that acquiring the data needed to power AI tools might require the use of vendors or other third-parties, which expands an entity's supply chain and could introduce security vulnerabilities that may be exploited by threat actors.

Controls and measures for mitigating AI-related threats

The Guidance notes that the 'Cybersecurity Regulation requires Covered Entities to assess risks and implement minimum cybersecurity standards designed to mitigate cybersecurity threats relevant to their businesses - including those posed by AI.' In other words, and as previously noted, the Guidance takes the position that assessment and management of cyber risks related to AI are already required by the Cybersecurity Regulation. The Guidance then sets out 'examples of controls and measures that, especially when used together, help entities to combat AI-related risks.' Specifically, the Guidance provides recommendations to Covered Entities on how to address AI-related risks in the context of implementing measures to address existing NYDFS requirements under the Cybersecurity Regulation. Although AI presents some cybersecurity risks, the Guidance notes that there are also substantial benefits 'that can be gained by integrating AI into cybersecurity tools, controls, and strategies.' It emphasizes that in order to ensure that countermeasures are sophisticated enough to meet the evolving threat of AI-related cybersecurity risks, Covered Entities must review and reevaluate their cybersecurity programs and controls at regular intervals, as they are required to do by the Cybersecurity Regulation.

- **Risk assessments and risk-based programs, policies, procedures, and plans** - Covered Entities should consider the risks posed by AI when developing risk assessments and risk-based programs, policies, procedures, and plans as required in the Cybersecurity Regulation. While the Cybersecurity Regulation already requires annual updates to risk assessments, the Guidance notes that these updates must ensure new

risks posed by AI are assessed. In addition, the Guidance specifies that the incident response, business continuity, and disaster recovery plans required by the Cybersecurity Regulation 'should be reasonably designed to address all types of Cybersecurity Events and other disruptions, including those relating to AI.' Further, the Guidance notes that the 'Cybersecurity Regulation requires the Senior Governing Body[1] to have sufficient understanding of cybersecurity risk management, and regularly receive and review management reports about cybersecurity matters,' which should include 'reports related to AI.'

- **Third-party service provider and vendor management** - The Guidance emphasizes that 'one of the most important requirements for combatting AI-related risks' is to ensure that all third-party service provider and vendor policies (including those required to comply with the Cybersecurity Regulation) account for the threats faced from the use of AI products and services, require reporting for cybersecurity events related to AI, and consider additional representations and warranties for securing a Covered Entity's non-public information if a third party service provider is using AI.
- **Access controls** - Building on the access control requirements in the Cybersecurity Regulation, the Guidance recommends that 'Covered Entities should consider using authentication factors that can withstand AI-manipulated deepfakes and other AI-enhanced attacks, by avoiding authentication via SMS text, voice, or video, and using forms of authentication that AI deepfakes cannot impersonate, such as digital-based certificates and physical security keys,' among other steps to defend against AI-related threats. The Guidance also advises Covered Entities to 'consider using an authentication factor that employs technology with liveness detection or texture analysis to verify that a print or other biometric factor comes from a live person.' Notably, the Guidance recommends, but does not require, Covered Entities to employ 'zero trust' principles and, where possible, require authentication to verify identities of authorized users for all access requests.
- **Cybersecurity training** - As part of the annual cybersecurity training requirements under the Cybersecurity Regulation, the Guidance suggests that the required training should address AI-related topics, such as the risks posed by AI, procedures adopted by the entity to mitigate these risks, and responding to social engineering attacks using

AI, including the use of deepfakes in phishing attacks. As part of social engineering training required under the Cybersecurity Regulation, entities should cover procedures for unusual requests, such as urgent money transfers, and the need to verify legitimacy of requests by telephone, video, or email. Entities that deploy AI directly (or through third party service providers) should also train relevant personnel on how to design, develop, and deploy AI systems securely, while personnel using AI-powered applications should be trained on drafting queries to avoid disclosing non-public information.

- **Monitoring** - Building on the requirements in the Cybersecurity Regulation to implement certain monitoring processes, the Guidance notes that Covered Entities that use AI-enabled products or services 'should also consider monitoring for unusual query behaviors that might indicate an attempt to extract [non-public information] and blocking queries from personnel that might expose [non-public information] to a public AI product or system.'
- **Data management** - The Guidance notes that the Cybersecurity Regulation's data minimization requirements, which require implementation of procedures to dispose of non-public information that is no longer necessary for business purposes, also applies to non-public information used for AI purposes. Furthermore, while recent amendments to the Cybersecurity Regulation will require Covered Entities to 'maintain and update data inventories,' the Guidance recommends that Covered Entities using AI should implement data inventories immediately. Finally, Covered Entities that use or rely on AI should have controls 'in place to prevent threat actors from accessing the vast amounts of data maintained for the accurate functioning of the AI.'

Risks of use of AI in financial services and regulatory enforcement trends

AI is not new in financial services - machine learning has been in play in the financial services sector for many years, including to monitor transactions for

fraud detection and anti-money laundering and to automate customer service interactions. Financial services are also a higher-risk industry more generally, not only in regard to AI-related cyberattacks that can threaten the broader financial infrastructure but also because of risks arising from the deployment of AI technologies in the financial sector and the implications for individual consumers. For example, common concerns about AI include concerns about data privacy, transparency of decision making, intellectual property, and discrimination and bias in automated systems, all of which can affect the rights of individual consumers when arising in the context of the provision of financial services.

Because of these heightened risks, regulators are scrutinizing the use of AI in the financial industry closely. The NYDFS is not alone emphasizing the importance of managing risks associated with the use of AI in financial services, and the Guidance sits among a growing pool of federal and state legislation and regulations that target these risks. For example, in response to Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (revoked by President Trump on January 20, 2025), the Department of Treasury issued its March 2024 report, Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector. The Consumer Financial Protection Bureau issued guidance regarding financial institutions' use of AI in denying credit. The Criminal Division of the U.S. Department of Justice updated its Evaluation of Corporate Compliance Programs policy document, requiring prosecutors to evaluate whether a company's compliance program includes safeguards to ensure that use of new technologies, including AI, will not result in 'deliberate or reckless misuse' violating criminal laws or the Company's Code of Conduct. Finally, the Securities and Exchange Commission (SEC) has highlighted AI disclosures as one of its examination priorities to ensure that companies are making statements that clearly define AI, specifying how and where AI is being used, and identifying the particular risks that the company faces from its use of AI.

In the absence of federal AI legislation and with uncertainty regarding the Trump administration's enforcement priorities regarding AI, states might assume a greater role in addressing AI risks. In addition to New York, other state legislatures are taking steps to regulate use of AI in the financial sector, introducing laws that layer additional risk considerations and proscribed risk-management practices onto those referenced by the Guidance. A number of these states have enacted laws that provide consumers with certain rights regarding automated decision-making. For example, the California Consumer

Privacy Act gives residents the right to opt out of the use of their personal information by automated decision-making technology, including for financial services, and requires pre-use disclosure of meaningful information about the logic involved in the automated decision-making process. The Colorado AI Act, enacted last year and scheduled to take effect in early 2026, more specifically targets AI discrimination. It classifies AI systems used for decisions in the financial services context, among others, as high risk, and thus subject to heightened regulatory obligations. Though the Colorado AI Act excludes certain banks or credit unions that are regulated by state or federal entities, in order to qualify for that exemption, banks or credit unions must be subject to guidance or regulations that are at least as stringent as the requirements of the Colorado AI Act and require the financial institution to regularly audit their use of high-risk AI systems for discrimination.

The risks and obligations surrounding the use of AI form a central component of corporate compliance, especially for entities operating in the financial sector. In light of the Guidance and the evolving state and federal regulatory landscape, Covered Entities, and other companies more broadly, will likely benefit from considering AI-related risks as part of their risk-management and governance programs.

Caleb Skeath Partner
cskeath@cov.com
Micaela R.H. McMurrough Partner
mmcmurrough@cov.com
Vanessa Lauber Associate
vlauber@cov.com
Covington & Burling LLP, Washington and New York

1. 'Senior Governing Body' is defined in §500.1(q) of the Cybersecurity Regulation as 'the board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer or officers of a covered entity responsible for the covered entity's cybersecurity program.'

Topics: Cybersecurity Artificial Intelligence

Jurisdictions: New York