eLANY

BULLETIN

Excess Line Association
Of New York

120 Wall Street, 24th Floor
New York, New York 10005

Bulletin No. 2024-22

November 4, 2024

RE: DFS LETTER ON AI AND CYBERSECURITY REGULATION

On October 16th, the Department of Financial Services ("DFS") issued a letter to executives and information security personnel at all DFS-regulated entities regarding **Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks**. Brokers and other regulated entities are advised to carefully review the letter in full. Here are some key takeaways:

- Whenever Risk Assessments are updated, Covered Entities should assess whether the identified risks warrant updates to cybersecurity policies and procedures in order to mitigate those risks.

- The incident response, business continuity, and disaster recovery plans should be reasonably designed to address all types of Cybersecurity Events and other disruptions, including those relating to AI.

- Covered Entities should require TPSPs to provide timely notification of any Cybersecurity Event that directly impacts the Covered Entity's Information Systems or NPI held by the TPSP, including threats related to AI. Moreover, if TPSPs are using AI, Covered Entities should consider incorporating additional representations and warranties related to the secure use of Covered Entities' NPI, including requirements to take advantage of available enhanced privacy, security, and confidentiality options.

- Covered Entities should consider using MFA 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. Similarly, instead of using a traditional fingerprint or other biometric authentication system, Covered Entities should 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. Another option is to use authentication via more than one biometric modality at the same time, such as a fingerprint in combination with iris recognition, or fingerprint in combination with user keystrokes and navigational patterns.

- Cyber training should ensure all personnel are aware of the risks posed by AI, procedures adopted by the organization to mitigate risks related to AI, and how to respond to AI-enhanced social engineering attacks.

- In addition, Covered Entities must provide training specifically designed for cybersecurity personnel. That training should include how threat actors are using AI in social engineering attacks, how AI is being used to facilitate and enhance existing types of cyberattacks, and how AI can be used to improve cybersecurity.

- If deploying AI directly, or working with a TPSP that deploys AI, relevant personnel should be trained on how to secure and defend AI systems from cybersecurity attacks, and how to design and develop AI systems securely. If other personnel are permitted to use AI-powered applications, they should be trained on how to draft queries to avoid disclosing NPI.

- Cyber Training should cover procedures for what to do when personnel receive unusual requests such as a request for credentials, an urgent money transfer, or access to NPI. For example, training should address the need to verify a requestor's identity and the legitimacy of the request if an employee receives an unexpected money transfer request by telephone, video, or email. Moreover, training should address circumstances in which human review and oversight must be included in verification procedures.

- Covered Entities that use AI-enabled products or services or allow personnel to use AI applications such as ChatGPT, should also consider monitoring for unusual query behaviors that might indicate an attempt to extract NPI and blocking queries from personnel that might expose NPI to a public AI product or system.

- If an entity uses AI or relies on a product that uses AI, controls should be in place to prevent threat actors from accessing the vast amounts of data maintained for the accurate functioning of the AI. In these cases, entities should identify all Information Systems that use or rely on AI, including, if applicable, the Information Systems that maintain, or rely on, AI-enabled products and services. These entities also should maintain an inventory of all such systems and prioritize implementing mitigations for those systems that are critical for ongoing business operations.

- Organizations should explore the substantial cybersecurity benefits that can be gained by integrating AI into cybersecurity tools, controls, and strategies.

If you have any questions, please email ElanyInfo@elany.org. Please ensure the domain elany.org is not blocked by your spam filter.