Treasury's Report on AI (Part 1) – Governance and Risk Management

April 29, 2024

On March 27, 2024, the U.S. Department of Treasury ("Treasury") released a report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector (the "Report"). The Report was released in response to President Biden's Executive Order ("EO") 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, which spearheaded a government-wide effort to issue Artificial Intelligence ("AI") risk management guidelines consistent with the White House's AI principles.

We recently hosted Todd Conklin, the Chief Artificial Intelligence Officer and Deputy Assistant Secretary of Cyber at Treasury, to discuss the Report. In Part 1 of this Debevoise Data Blog series, we address the Report's coverage of the state of AI regulation and best practices recommendations for AI risk management and governance. Part 2 will cover the Report's assessment of uses of AI in cybersecurity and fraud protection, AI cybersecurity risks, cybersecurity best practices recommendations, and challenges and opportunities for the financial sector.

REPORT SCOPE, METHODOLOGY, AND DEFINITIONS

The Report is a digest of AI use cases, threat and risk trends, governance and cybersecurity best practice recommendations, and challenges and opportunities for financial institutions. To obtain a comprehensive understanding of AI use in the financial sector, Treasury conducted 42 in-depth interviews with a broad range of industry stakeholders, including financial institutions, trade associations, IT firms, data providers, payment service providers, cybersecurity and anti-fraud companies that use AI features in their services, and regulatory advocacy groups.

The Report adopts the definition of AI set forth in the EO.[1] Notably, however, interviews revealed that there is no common AI lexicon—participants disagreed about

[1] "The term 'artificial intelligence' or 'AI' has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions

the meaning of "AI" and other terms, including "hallucination," and "prompt" or "response," as well as the appropriateness of the use of these terms when applied to this technology.

EXISTING REGULATORY LANDSCAPE AND BEST PRACTICES

In its Report, Treasury outlines the current regulatory landscape applicable to the use of AI in cybersecurity and fraud management by financial services firms. These regulatory expectations, in turn, closely track best practices shared by participating financial institutions for mitigating AI-related cyber and fraud risks.

Designing and Implementing AI Risk Management Frameworks

Participating financial institutions reported adopting different approaches to designing the structure and substance of AI risk management frameworks.

- **Structure**: The Report highlights two structures interviewed stakeholders recommended for AI risk management frameworks.
  - **Vertical integration**. This approach vertically integrates AI risk management within the broader enterprise risk management program, along three "lines of defense." The first line, the business line, is responsible for managing risk associated with the use of AI in business offerings. The second line is the corporate risk management line, which supports the business line with compliance management systems and risk management structures and escalates information and decisions to management. The third line, audit, ensures that appropriate monitoring, controls, and reporting structures are in place.
  - **Principles-based approach**. In the alternative, the NIST Risk Management Framework ("RMF") suggests a principles-based approach, where senior leaders determine overall goals, values, and policies for enterprise risk and design AI risk management frameworks to implement such principles.
- **Substance**: Interviewed financial institutions reported that they developed such AI risk management frameworks by adapting existing guidelines such as NIST's RMF, OECD AI Principles, and Open Worldwide Application Security Project AI Security

influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."

and Privacy Guide. However, other participants reported developing bespoke approaches by leveraging existing principles.

Whatever approach taken, the Report advises that financial institutions implement AI risk management frameworks by:

- **Ensuring sufficient coverage**. AI risk management frameworks should be implemented to address risks throughout the AI life cycle, across the enterprise.

- **Establishing accountability through transparency**. Transparency is necessary to ensure accountability for AI risk management. Best practices such as inventory, appropriate documentation, and effective communication can enhance transparency.

- **Mapping AI risks against existing controls**. Companies should consider mapping AI risks against existing controls across the enterprise, to ensure gaps can be addressed.

Governance

The Report advises that implementing effective AI risk management frameworks requires appropriate AI governance, including:

- **Designating AI governance lead(s)**. Participating institutions have taken different approaches to assigning responsibility for AI governance. Some organizations have assigned responsibility to a single lead official, like the Chief Technology Officer or Chief Information Security Officer. Other institutions have designated responsibility to an AI center of excellence, or the board of directors.

- **Ensuring cross-functional and cross-team collaboration**. Given the diversity and complexity of risks associated with AI, the most common approach has been to integrate AI risk management across functions, including model risk, technology risk, cybersecurity risk, and third-party risk management, and teams, including legal, compliance, data science, marketing, and business functions.

Data Management

Complex data supply chains power AI systems. Given the complexity and diversity of these supply chains, interviewed financial institutions reported the following best practices for data management:

- **Mapping data supply chain**. As more key functions rely on AI systems, certain financial institutions are inventorying their data supply chain, to track data provenance, lineage, transformation, and integration.

- **Designating a corporate data lead**. This mapping is typically coordinated by a corporate data lead, who also participates in cross-functional AI risk management, streamlines data requirements across the enterprise, and drives innovation through data. The corporate data lead is often the Chief Data Officer.

Vendor Management

Vendors that offer AI systems or products or services relying on AI systems pose additional financial, legal, and security risks. To account for AI risks, the Report advises that financial institutions consider:

- **Expanding third-party due diligence and monitoring to account for AI risks**. Including due diligence questions regarding the third-party's use of AI technologies, data privacy and retention policies, AI model validation and maintenance procedures, and reliance on and management of other vendors for data or models may assist financial institutions with managing vendor risks. Existing resources, including the Financial Services Information Sharing and Analysis Center's *Generative AI Vendor Evaluations & Qualitative Risk Assessment Guide*, may be helpful for financial institutions to consult in developing these procedures.

Implementing AI Systems

In its Report, Treasury observes that enterprise IT system developers and practitioners may be pressured to capitalize on recent advancements in AI, particularly generative AI. But new technologies present new shortcomings—before buying into hype and onboarding new AI systems or augmenting existing systems with AI functionalities, the Report advises that financial institutions consider:

- **Risk-assessing new systems before determining whether or how to use AI**. Certain AI systems may present inherently greater risks and challenges for implementation. For example, if implementation requires explainability, generative AI may not be a viable option. Financial institutions should assess vendors or systems based on their capabilities, fit-for-purpose, and limitations, to determine whether or how to use AI systems.

- **Applying existing cybersecurity best practices**. Financial institutions should map security controls to AI systems and data and ensure that they are subject to at least the same levels of cybersecurity as other IT systems.

* * *

The Report is part of Treasury's ongoing project to examine the impact of AI on financial services. It concludes with a list of proposed next steps that Treasury, other

agencies, regulators, and the private sector could take to address the risks discussed above. These include: (i) aligning on common terminology specific to AI; (ii) addressing the capability gap between financial institutions of varying sizes when it comes to developing AI systems; (iii) and enhancing coordination among regulators.

In the meantime, financial institutions should prepare for further regulatory development by adopting best practices identified in the Report for managing the opportunities and risks posed by the use of AI in the financial sector.

To subscribe to the Data Blog, please click here.

The cover art used in this blog post was generated by DALL-E.

* * *

Please do not hesitate to contact us with any questions.

Charu A. Chandrasekhar
Partner, New York
+1 212 909 6774
cchandra@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

Johanna Skrzypczyk
Counsel, New York
+1 212 909 6291
jnskrzypczyk@debevoise.com

Michelle Huang
Associate, New York
+1 212 909 6553
mhuang1@debevoise.com

Sharon Shaji
Law Clerk, New York
+1 212 909 7458
sshaji@debevoise.com

Annabella M. Waszkiewicz
Law Clerk, New York
+1 212 909 7484
amwaszki@debevoise.com