Contribution to NIST's second draft of the AI RMF

Mastercard welcomes the opportunity to share its views with the National Institute of Standards and Technology on its proposed AI Risk Management Framework (RMF) presented as a second draft on 18th August 2022.

As NIST may be aware, the financial services industry was an early adopter of AI and machine learning. At Mastercard, our approach to AI development has been built on a set of data responsibility principles around privacy and security, to guide innovation and the development of our own AI Governance framework. Our implementation of these principles ensures the necessary safeguards are in place for subject-oriented[1] and responsible AI. At a moment of increased vulnerability across the economy, AI-based tools, built on a robust governance framework, have helped Mastercard facilitate access to the digital economy, thus increasing trust in our payment network and solutions.

We welcome the development of the AI RMF, which contains insights that Mastercard will most certainly draw inspiration from to enhance our own practices, and in this context, we would like to respectfully share our reflections on the draft RMF with the National Institute of Standards and Technology. We provide below some general observations and some specific proposed amendments to the text:

General Observations

Extending the RMF to cover the full lifecycle of AI

The extents of the proposed RMF do not fully match the stated purpose to "cultivate trust by understanding and managing the risks of AI systems." Mastercard would suggest that the AI RMF be amended to more explicitly cover the decision-making-process (DMP) that leads to the decision to use AI in a product, service, or process. The decisions to use AI, and around how to deploy and implement are based on a contextual desire to increase efficiency, reduce costs, and/or improve effectiveness of a process. The DMP involves a choice between technologies or human versus machine operations. That DMP should form

[1] Subject-oriented AI refers to an approach to always consider the subject of the AI at every stage of the design process, whether it applies to humans (human-centric AI), manufactured goods or the weather, the subject of the AI should be the focal point during development of the model

part of the RMF with audits considering the appropriateness of the DMP and the effectiveness of the oversight applied to such decisions.

Selection of the AI model type

The RMF should take into consideration that as AI becomes more democratized the selection of the AI model may be undertaken by individuals without a deep understanding of AI. Modern software packages are enabling non-practitioners to apply thousands of models to a training dataset and select the model with the best fit. Advances in no-code AI and automatic ML (e.g., Microsoft Automatic ML, IBM AutoAI, and Amazon Sagemaker AutoPilot) have enhanced workflows and the adoption of AI. Even skilled practitioners are now presented with so many different models and AI techniques that it is impossible to understand the limitations or risks with each specific model. This risk is covered quite well by the FRB (Federal Reserve Bank) Supervisory Guidance SR 11-7, so we would suggest a reference could be made to that standard by way of explanation and mitigation for the risk.

Organizational risk appetite

The RMF makes several references to AI risk fitting within organizational risk processes. Further, the RMF suggests that organizational risk varies and is situational (contextual and use-case specific). However, many organizations, including Mastercard, have a defined and published risk appetite that includes a defined volatility range, acceptable levels of uncertainty and procedures as to how to seek approval to go beyond these thresholds. It would be advantageous if the RMF gave guidance on how to manage situational AI risk within a pre-defined organizational risk appetite. Mastercard would be happy to engage in this area.

AI within the supply chain

An area of growing importance for Mastercard is the ongoing monitoring, assessment, and audit of AI within our supply chain. Whilst the RMF Govern section recognizes the need to have policies in place for AI in supply chains, there is a substantial amount of potential risk within supply chains. This ranges across business services for finance, human resources and marketing, through to product supply chains, such as fraud detection, financial inclusion, supporting start-ups, and customer rewards. Mastercard would be pleased to share experiences of managing AI in our supply chain and the journey we are still on.

In addition, larger supply chains contain systemic risks due to circular data re-use, which can manifest itself in several sections of the supply chain using the same data to test or validate the models and multiple models feeding off the same data. This is particularly problematic when third parties are involved in the supply chain.

Definition of actors and production stages

NIST has aligned to the Organization for Economic Co-operation and Development (OECD) defined AI lifecycle. Further, NIST has indicated that The Resource Center will provide a knowledge base, including terminology and terms used by different AI stakeholders. We recommend that the framework also address gaps in existing processes and nomenclature used by various actors throughout the AI Lifecycle, examples include differences between ML Ops terminology, model risk management, data science, etc.