Data and Operational Risk

July 2022

As financial service firms seek to use an expanding universe of data in increasingly sophisticated ways, a fragmented regulatory landscape is raising barriers while at the same time, firms are grappling with new dimensions of risk. The latest session of DataTalk explored the impact of data frameworks on operational resilience and was held in collaboration with the IIF Regulatory Affairs team. The call covered key themes that we are addressing through a joint effort between the Digital Finance Working Group and the Special Committee on Effective Regulation (SCER). This note provides a summary of the discussion, respecting that the conversation was conducted under the Chatham House Rule and comments are unattributed.

Operational Risk is conceived of differently around the world. Regulators, financial institutions, and third-party service providers have different concepts of what a resilient operation may look like. Many regulators are focused on financial stability, while several financial institutions are looking to maintain continuous service in the event of a disruption or security event. As a result, concentration risk is thought of differently among these groups. There are also localization requirements that seek to separate group-level activities from those in local entities. This fragmentation also introduces new operational challenges and risks. Participants agreed on the need for greater dialogue between these types of actors to reach a common understanding in service of smart regulation in this space.

The need for regulatory clarity remains pressing, as fragmentation poses a growing threat to the future of finance. Participants are already managing conflicts between regulatory regimes, and increasingly, regulatory conflict between agencies within one jurisdiction, as different authorities have taken different approaches to regulating activities, risks, entities, or assets. Principles-based and risk-based models for regulation offer the best path forward to coordinate standards across markets.

Data restrictions, such as limits on cross-border data flows, have created a fragmented regime. These silos are raising costs and limiting innovation. Limits on data flows are also emerging as an issue within markets, as different regulators ask for different types of protections. Even efforts which use proxy data—created by algorithms to distance analyzed data from the underlying personal information—still result in delays and limit applications. Such silos create barriers to entry, slow the growth of the space, and increase the concentration of firms engaged in these business lines.

Scale matters in more than one sense. The additional compliance lift of adhering to reporting requirements and security measures in each jurisdiction, along with the resources needed to understand different regulatory asks, is preventing smaller firms from gaining a foothold in the FinTech space. Large firms have the resources to sort through these differing protection regimes, while small firms do not. Licensing requirements add an additional burden. To reduce these barriers, DataTalk participants suggest focusing on three things: 1) prioritizing fraud and criminal detection in data standards and sharing agreements; 2) setting clear, but different, standards for security and usage limits depending on the type of activity; 3) smoothing access for product development through sandbox or limited trail usage regimes.

We look forward to continuing the DataTalk series in August, when we will discuss AI, data frameworks, and new regulation with a focus on the implications for the insurance industry.