How crisis-proof are financial market infrastructures?

Apostolos Thomadakis*

The pandemic has caused unprecedented volatility in the financial markets. The corporate sector has been hit by supply disruptions and weak demand. Amid such turbulence, providers of infrastructure services for financial markets, such as exchanges, clearinghouses, trade depositories and custodians, financial data, and technology providers, are vital to providing robust and stable platforms and operations as well as timely information to allow for efficient transactions. Their operational resilience should enable them to go on contributing to well-functioning secondary markets and ensure the recapitalisation of primary markets.

- What risk-management tools do market infrastructure providers have to deal with the unprecedented crises? Has their effectiveness been tested?
- Are national ecosystems sufficiently integrated across the EU? Has interoperability been achieved in practice?
- Is the current regulatory framework protecting the financial sector and wider economy from potential operational disruptions?
- Are capital markets and the financial sector structured in a way that could prevent, adapt, respond to, recover, and learn from operational disruptions?

Speakers:

Carmine Di Noia, Commissioner, CONSOB & Chair, Committee for Economic and Markets Analysis, ESMA
Boris Augustinov, Policy Officer, Digital Finance Unit, DG FISMA, European Commission
Rachel Tyler, Executive Director of Business Resiliency, DTCC
Mark Spanbroek, Chairman, FIA EPTA

Moderated by **Karel Lannoo**, CEO of CEPS and General Manager, ECMI

* *Apostolos Thomadakis is Researcher at ECMI and CEPS.*

The report is not a transcript of the speakers' interventions; rather, it should be understood as an interpretation of their views by the author.

Summary

The resilience of financial market infrastructures has been a much-debated issue in recent years, and perhaps never more so than since the beginning of the Covid crisis and the market crash last March. Covid was a big stress test for all market infrastructures at all levels, but they managed to navigate through the storm and remain resilient. Their business model has proved to be adaptable and flexible enough to cope with the transition from a physical to a completely virtual mode overnight, and communication with regulators and policymakers was efficient. Furthermore, capacity shortage problems such as those that happened during the 2004-05 terrorist attacks (in Madrid and London) and the global financial crisis did no recur.

However, uncertainty about keeping the markets open, threats of short-sale bans and the non-harmonised response of European regulators could have been avoided as they can affect stability, create liquidity shortfalls and impose unnecessary risks. Moving forward, there is a need for better coordination among supervisors, the harmonisation of procedures and reporting requirements, the creation of a roadmap/rulebook on how market infrastructures should react and respond to extreme events, and the creation of a minimum baseline that would boost the operational resilience of the financial sector.

The regulatory focus on resilience has shifted significantly over the years. What started out as geographical dispersion to prevent disruption of service for natural disasters and physical events became financial and cyber resilience, while is now called more broadly operational resilience. After the global financial crisis, regulators focused more on traditional risks (e.g. market risk, liquidity risk, credit risk) and significantly less on operational risks – which include both ICT (Information and Communication Technology) (e.g. communication equipment, hardware and software) and non-ICT (e.g. machinery and equipment, and non-residential buildings) components. Nowadays, however, nowadays, financial market infrastructures are almost fully dependent on ICT components.

It is important to distinguish between business resilience and operational resilience.[1] The former can be defined as an overarching concept that refers to an organisation's ability to safeguard its critical business services against the threat of potential disruptive events, regardless of their nature. On the other hand, the latter – which is a part of business resilience alongside financial and technical resilience – refers to the people in the processes supporting the critical services and the governance surrounding them.

The Covid-19 pandemic had, and continues to have, not only a health/physical dimension, but also a technological/cyber one. Cyber is very different from the physical world because the threats are constantly changing and there are many unknowns. A cyber threat can be defined as an event where data is either lost or corrupted in such a way that a firm cannot trust it and it cannot trust the output from its processes. Such a major event has no easy answer, given that a firm can only try to make the best possible decision with the limited information available. The actions taken by a firm in a cyber-event (e.g. the decision to remove a participant from the ecosystem) could have far-reaching implications due to the interconnectedness of the marketplace. Furthermore, performing large-scale

[1] See DTCC, "Resilience First: Promoting Financial Stability by Planning for Disruption", September 2019.

testing is very challenging, given that no one wants to introduce such a threat into their environment. Testing is therefore mostly tabletop and procedural rather than actual execution.

The structure of financial markets has evolved significantly over the last 30 years. There is considerable growth in exchanges, both in terms of size and their role in the financial system, while their corporate governance structure has shifted from mutual non-profit or public entities towards a listed company model. The number of listed companies is on a steady decline, following the global trend, and there is a more vertical integration across products than used to be the case 10 or 20 years ago. Technology has also advanced and has been widely adopted, playing a fundamental role in the functioning of financial markets.

During the Covid-19 crisis, financial institutions have been resilient to both the downturn and the upswing in the market. Their resilient business model allowed them to switch from no remote at all to completely remote virtually overnight. Thankfully, there was no exchange outage during the crisis in March as this would have been an extreme and severe test. Communication with regulators and policymakers functioned very well.

The Commission's new initiative, DORA (Digital Operation and Resilience Act), which did not attract much attention because it was launched on the same day as the new CMU action plan, is an essential legislative proposal aimed at digital operational resilience. This is because market infrastructure and market participants need to be sure there is reliability and resilience to shocks that come from new exogenous sources not identified in the past (e.g. health, environmental, social, and cyber-attack risks).

Building on the many work streams at European and international level, the principle-based approach of DORA aims to streamline the provisions/requirements of the financial legislation and create a minimum baseline to boost the digital operational resilience of the financial sector. It covers almost the entire financial sector and addresses five main areas that are relevant from a digital operational resilience perspective: i) ICT risk management; ii) incident reporting; iii) testing; iv) third-party risk; and v) information sharing.

Importantly, proportionality has been embedded in the rules and addressed by specific exemptions. For example, certain provisions do not apply to microenterprises, while some rules are only applicable to significant institutions (e.g. the threat led penetration testing and the reporting of incidents are only for major ICT related incidents). As for the supervision of the application of DORA, this is down to the competent authorities responsible in the sectoral legislation.

Moving forward, and from a regulatory perspective, there are certainly areas of opportunity, particularly with respect to harmonisation, definitions, and reporting requirements. In 2019, for example, according to the latest ESMA data, there were 430 platforms (regulated markets, multilateral trading facilities, organised trading facilities) and 216 systematic internalisers operating in Europe. Although these numbers increase year on year, liquidity comes from only three or four trading platforms. Furthermore, there are far too many different approaches to the same issue, which keeps markets uncertain and market operators on the sidelines. Equally, the lack of a consolidated tape adds a layer of uncertainty for investors as they are unable to see the true price (i.e. liquidity) of a product.

Despite that level of fragmentation, it should be acknowledged that even though firms offer critical business services, not all services are as critical all the time. For example, a payment service could be more critical on a day that is a high principal and interest payment day, but not on a day that isn't. Similarly, from an underwriting perspective, a big IPO issuance day is far more critical for the underwriting service than any other ordinary day.

Having said that, firms and financial infrastructures should continue to plan for physical events, while looking at cyber and maintaining service objectives. To achieve that, they should: i) design for resilience by planning for failure (e.g. understand interactions between business services, supporting processes, documenting agreed policies and procedures); ii) assess the resilience of the ecosystem (e.g. impact to client, reliance on third parties); iii) monitor resilience (e.g. tracking the robustness of processes, maintaining intelligence, developing metrics); and iv) continuously test resilience capabilities (e.g. test resilience-related processes, ensure the thorough understanding of policies and procedures, improve the ability to measure, monitor and manage risks).

European Capital Markets Institute

ECMI conducts in-depth research aimed at informing the debate and policy-making process on a broad range of issues related to capital markets. Through its various activities, ECMI facilitates interaction among market participants, policymakers and academics. These exchanges are fuelled by the various outputs ECMI produces, such as regular commentaries, policy briefs, working papers, statistics, task forces, conferences, workshops and seminars. In addition, ECMI undertakes studies commissioned by the EU institutions and other organisations, and publishes contributions from high-profile external researchers.

Centre for European Policy Studies

CEPS is one of Europe's leading think tanks and forums for debate on EU affairs, with an exceptionally strong in-house research capacity and an extensive network of partner institutes throughout the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research that addresses the challenges facing Europe and to maintaining high standards of academic excellence and unqualified independence and impartiality. It provides a forum for discussion among all stakeholders in the European policy process and works to build collaborative networks of researchers, policymakers and business representatives across Europe.