SPECTRUM®

THREATS TO THE ORDERLY FUNCTIONING OF A NETWORK OF VENUES

by Alpay Soytürk, Spectrum Markets

The importance of trading venues for the financial system is a rather subliminal perception, at least most of the time. "These outstretched hands" as the German economist and sociologist Max Weber[1] wrote in 1894, referring to supply and demand, "must be able to meet, and the market is essential for this". While there's little resemblance left between the economies of the late 19th century and today's, Weber's references to price discovery and price formation are timeless.

People do not necessarily have in mind macroeconomic relationships when thinking of trading venues, but everyone envisions their relevance when things don't work as they normally do. If markets get nervous and if there are exaggerations in either direction, that is devastating enough. But when trading venues are out of service as a result of technological inadequacies, this is a threat to investor confidence and market integrity. When referring to exchange outages, the first thing that comes to mind is the extraordinary volatility throughout March 2020 that stretched many market infrastructures to their limits, some even beyond.

However, in its TRV Report[2], the European Securities and Markets Authority (ESMA) did not point at this ultra-high volatility period in the first quarter of 2020, when the number of circuit breaker trigger events reached 3,300 per week on average. The technological issues that ESMA considered as having posed "threats to the orderly functioning of a network of venues" occurred in the second half of 2020 when circuit breaker[3] trigger events had declined to less than 80 per week. According to ESMA, the real concern is about an increased reliance on third-party data or software providers and cloud services.

It is important to note that authorities are not criticising the outsourcing of certain business functions as such; regulated entities have been employing third party providers for many years. There is even dedicated regulation existing around how relevant processes have to be structured and governed. In essence, the more critical the service concerned the more rigorous are the requirements attached to its outsourcing.

For most of the time, this has worked well and initial fears – mainly in the context of cybersecurity – have given way to the recognition of the many benefits associated with the outsourcing services. Beyond saving on infrastructure expenditure, outsourcing offers more control over IT running costs due to the significant flexibility surplus in comparison with on-premise deployments. This flexibility includes the easier scalability of capacities, cheaper adaption of the latest software standards and a greater overall level of standardisation throughout the industry. Last but not least, safeguarding a network from cyberattacks or from technological risks in association with capacity or redundancy is mostly much more effectively managed by cloud service providers than firms could arrange for themselves.

> "There's no quick fix to reassuring clients and regulators that it will be OK next time. Technology changes have long lead times and, once implemented, it takes time to regain trust."

According to a survey by Gartner[4], public cloud service revenues will have reached a volume of USD 331 billion by 2022, almost double the spending of the USD 182 billion in 2018. These services include Cloud Business Process Services (BPaaS), Cloud Application Infrastructure Services (Platform as a Service, PaaS), Cloud Application Services (Software as a Service, SaaS), Cloud System Infrastructure Services (Infrastructure as a Service, IaaS) and other cloud management and security services. BPaaS are automated business processes delivered from a cloud service. PaaS provide a cloud-based environment for developing, testing, delivering and managing software applications such as MS Azure or IBM Cloud. SaaS are apps deployed in the cloud such as Microsoft 365. IaaS provides the usage and management of IT infrastructure over the internet on pay-per-usage basis with Amazon's AWS being the most prominent example. The top five public cloud companies are thought to earn over three-quarters of the total public cloud infrastructure revenues.

But if cloud services rank better than most firms' proprietary IT operations in terms of costs, flexibility security and so-on, what's the catch? According to the supervisory authorities, the concern is the over-reliance on the Cloud Service Providers rather than the usage of such services in general. This over-reliance prevails, although there is not a lack of regulatory guidance as to how risk management responsibilities are to be divided or shared between providers and users of cloud services. For entities such as Regulated Markets or Multilateral Trading Facilities there are, among others, the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) which lists standards for entities that outsource some operations to another market infrastructure or a third-party service.

With technology progressing fast and more and more processes being assigned to external partners, outsourcing entities are not only at risk of falling behind in terms of expertise in wider areas of IT infrastructure; they tend to believe that what's outsourced ultimately falls within the sole sovereignty of the service provider. Irrespective of this legal misconception, outages, even if rare, do occur even at large providers.

In its TRV Report ESMA has cited a number of outages during 2020, some of which resulted in unpleasant outcomes for the end investor or the functioning of an entire market. However, the question must be raised whether these outages were in fact attributable to outsourcing.

A report[5] by the Financial Stability Board admits that outages at Cloud Service Providers, if they occur, mostly don't last very long (mostly just for minutes) and that redundancy is rarely a concern in that context. Be that as it may, even if outages can't be eliminated entirely, the ultimate responsibility for the seamless operation of a market infrastructure rests with the operator of that market – and the more outdated the technology is used, the more difficult it will be to safeguard system uptime.

Recently some market participants raised the idea of responding to outages by establishing a mutual back-up operation mode between venues. If such plans ever materialise and, more importantly, whether they will prevent outages remains to be seen. Or, as our CEO, Nicky Maan told the Financial Times in May, "There's no quick fix to reassuring clients and regulators that it will be OK next time. Technology changes have long lead times and, once implemented, it takes time to regain trust."

---

[1] Maximilian Carl Emil Weber (* 21.4.1864 † 14.6.1920), „Die Börse", 1894

[2] TRV 1.2021 ESMA Report on Trends, Risks and Vulnerabilities

[3] Trading halts or constraints on limit order books that trip when pre-defined thresholds are reached during a trading session aiming at cooling-down trading, allowing an auction to pool liquidity and curb volatility

[4] "Forecast: Public Cloud Services, Worldwide, 2016-2022"

[5] "Third-party dependencies in cloud services – Considerations on financial stability implications"

Get in touch today to discuss how we can help you to grow your retail client business.

Please don't hesitate to get in touch if you wish to receive further detail.

spectrum-markets.com

Dr. Alpay Soytürk, LL.M.
Head of Compliance and Surveillance
+49 69 427 299 192
Alpay.Soyturk@spectrum-markets.com