THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

TECHNOLOGY

COVID-19 shines a spotlight on the reliability of the financial market plumbing

UMAR FARUQUI | JENNY HANCOCK

20 YEAR ANNIVERSARY

OPERATIONAL RESILIENCE

#53 MAY 2021

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

OPERATIONS

TECHNOLOGY

MILITARY

DEAR READER,

Welcome to this landmark 20th anniversary edition of the Capco Institute Journal of Financial Transformation.

Launched in 2001, the Journal has followed and supported the transformative journey of the financial services industry over the first 20 years of this millennium – years that have seen significant and progressive shifts in the global economy, ecosystem, consumer behavior and society as a whole.

True to its mission of advancing the field of applied finance, the Journal has featured papers from over 25 Nobel Laureates and over 500 senior financial executives, regulators and distinguished academics, providing insight and thought leadership around a wealth of topics affecting financial services organizations.

I am hugely proud to celebrate this 20th anniversary with the 53rd edition of this Journal, focused on 'Operational Resilience'.

There has never been a more relevant time to focus on the theme of resilience which has become an organizational and regulatory priority. No organization has been left untouched by the events of the past couple of years including the global pandemic. We have seen that operational resilience needs to consider issues far beyond traditional business continuity planning and disaster recovery.

Also, the increasing pace of digitalization, the complexity and interconnectedness of the financial services industry, and the sophistication of cybercrime have made operational disruption more likely and the potential consequences more severe.

The papers in this edition highlight the importance of this topic and include lessons from the military, as well as technology perspectives. As ever, you can expect the highest caliber of research and practical guidance from our distinguished contributors. I hope that these contributions will catalyze your own thinking around how to build the resilience needed to operate in these challenging and disruptive times.

Thank you to all our contributors, in this edition and over the past 20 years, and thank you, our readership, for your continued support!

Lance Levy, **Capco CEO**

COVID-19 SHINES A SPOTLIGHT ON THE RELIABILITY OF THE FINANCIAL MARKET PLUMBING

UMAR FARUQUI | Member of Secretariat, Committee on Payments and Market Infrastructures, Bank for International Settlements (BIS)[1]
JENNY HANCOCK | Member of Secretariat, Committee on Payments and Market Infrastructures, Bank for International Settlements (BIS)

ABSTRACT

COVID-19 has shone a light on how dependent we are on the financial market plumbing. Despite the sudden and extended move to remote working, the plumbing has generally continued to operate as expected. Typically, the expectation is that the plumbing is available at least 99.9 percent of the time, and if there is an incident that it is fixed within two hours. Despite the combination of remote working and heightened market activity, the number and duration of outages was largely unchanged. In the early stages of the pandemic, increased volumes did lead to minor operational hitches and there were pressures from larger and more frequent margin calls at central counterparties – but generally the infrastructure continued to operate as expected. Nevertheless, COVID did bring to the fore a number of known challenges that require further consideration. It will be important for the infrastructure and the relevant authorities to use the COVID-19 pandemic as an opportunity to learn and further improve the resilience of the financial market plumbing. If they do, users can go back to assuming that when we turn on the tap, financial assets will flow freely through the (financial market) plumbing as expected.

1. INTRODUCTION

COVID-19 reignited interest in wastewater surveillance as a way to track and identify the spread of the disease [Forbes (2021)]. In the world of finance, there was also renewed interest in the so-called "plumbing" – financial market infrastructures (FMIs).[2] Financial market infrastructures are entities such as payment systems, central counterparties (CCPs), central securities depositories, and securities settlement systems, which ensure that funds and assets are able to move around in a safe and efficient manner. Just like with real world plumbing, no one in the street really thinks or cares about how the system works – until it does not.

While operational problems at FMIs are rare, they do occur. Some recent examples include:

- In February 2021, an "operational error" led to Fedwire Funds Services[3] being unavailable for some hours [Kiernan (2021)].
- In October 2020, an incident at TARGET2[4] resulted in all settlement services being unavailable for almost 10 hours. This also affected the securities settlements and instant payments that are linked to TARGET2. An initial investigation determined that a software defect in a network device caused the incident [ECB (2020a), ECB (2020b)].

[1] The authors would like to thank Takeshi Shirakami for helpful comments and suggestions, and Ilaria Mattei for excellent research assistance. The views expressed in this article are those of the authors and not necessarily the views of the BIS or the Committee on Payments and Market Infrastructures (CPMI).
[2] A financial market infrastructure is defined as a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions (CPMI Glossary; https://bit.ly/3fhu0FI). Financial market infrastructures comprise central counterparties, payment systems, securities settlement systems, central securities depositories, and trade repositories.
[3] Fedwire Funds Services is an electronic funds-transfer service in the U.S. and is used for inter-bank transactions.

- In September 2020, an internal technical issue resulted in intermittent outages at CREST.[5] Among other things, the outage impacted gilt sale and purchase operations by the British government [Reuters (2020)].
- In August 2018, a problem with the configuration setting in the Danish large-value payment system (KRONOS) led to multi-day delays in payment of salaries and transfers [DN (2018)].
- In August 2018, a disruption to the power supplying one of the Reserve Bank of Australia's data centers led to a outage of both the real-time retail payment system and the wholesale payments system in Australia. While real-time retail payment services were restored after three hours, it took almost eight hours to fully restore wholesale payment services [RBA (2019)].
- In June 2018, an outage of the Visa Europe card authorizations system prevented many customers from using their debit and credit cards for up to ten hours and affected 2.4 million Visa transactions that were attempted on U.K.-issued cards during that time [BoE (2019)].

If it is perceived among the general public that operational issues at financial market infrastructures have been uncommon it is, in large part, because of recognition by authorities of their critical role in the economy and the high standards that these entities are expected to adhere to both in normal times and – even more importantly – crisis periods, including pandemics.

During the COVID-19 pandemic, financial market infrastructures have had to deal with two major operational challenges: the move to business continuity operations and increased activity due to market volatility. Financial market infrastructures have generally coped well with these challenges and without major disruptions to the financial system. However, some operational issues remain, which will require continued vigilance from both financial market infrastructures and authorities.

The rest of this article describes the operational risk management requirements for financial market infrastructures set out in international standards, explains the challenges that COVID-19 has posed for financial market infrastructures and how they have responded, and outlines the ongoing challenges.

2. OPERATIONAL RISK MANAGEMENT REQUIREMENTS FOR FMIS

The Principles for Financial Market Infrastructures (PFMI), issued by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO), set out international standards for managing risks and ensuring efficiency and transparency at systemically important financial market infrastructures [CPMI-IOSCO (2012)]. These standards cover operational resilience, including business continuity management. Jurisdictions that are members of the CPMI or the IOSCO board are expected to implement these expectations in their legal and regulatory or oversight frameworks. CPMI-IOSCO also have a rigorous program for assessing the consistent implementation of the PFMI across jurisdictions and to examine the consistency of outcomes at financial market infrastructures.[6]

The Principles for Financial Market Infrastructures define operational risk as the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by a financial market infrastructure. Principle 17 of the Principles for Financial Market Infrastructures sets out expectations regarding the systems, policies, procedures, and controls financial market infrastructures have to implement to mitigate operational risk.

A financial market infrastructure's systems are expected to be designed to ensure a high degree of security and operational reliability and have adequate, scalable capacity. To achieve this, the Principles for Financial Market Infrastructures expect financial market infrastructures to establish a robust risk management framework to identify, monitor, and manage operational risks, including clearly defined operational reliability objectives. For example, central counterparties target operational availability of at least 99 percent, and typically 99.9 percent or more (Figure 1, left-hand panel). For a central counterparty that operates 9am to 5pm, five days a week, this translates to outages totaling no more than one hour in a year.[7]

While financial market infrastructures' systems are designed to be reliable, they are also expected (under the Principles for Financial Market Infrastructures) to have business continuity plans to respond to disruptions, including events that could

[4] TARGET2 is the payment system owned and operated by the Eurosystem used to settle payments related to the Eurosystem's monetary policy operations, as well as interbank and commercial transactions.
[5] CREST is the central securities depository for equity and bond markets in the U.K.; it is owned and operated by Euroclear U.K. and Ireland.
[6] Reports on the outcome of this implementation monitoring are published here: Monitoring implementation of the PFMI (bis.org), https://bit.ly/31gfrKq.
[7] This would be even less once public holidays are taken into account.

cause a wide scale or major disruption. Amongst other things, these plans are expected to cover a pandemic scenario. In developing these plans, a financial market infrastructure should aim to be able to resume operations within two hours, or at least complete settlement by the end of the day of the disruption, even in extreme circumstances. Financial market infrastructures are expected to regularly test their business continuity arrangements.

A core part of a financial market infrastructure's business continuity plan is a secondary site that can take over operations from the primary site if needed. Indeed, some financial market infrastructures have more than one backup site to provide additional resilience. To facilitate business continuity, critical IT systems are replicated at the backup site(s) and there needs to be appropriate staffing arrangements that would not be affected by a wide-scale disruption.

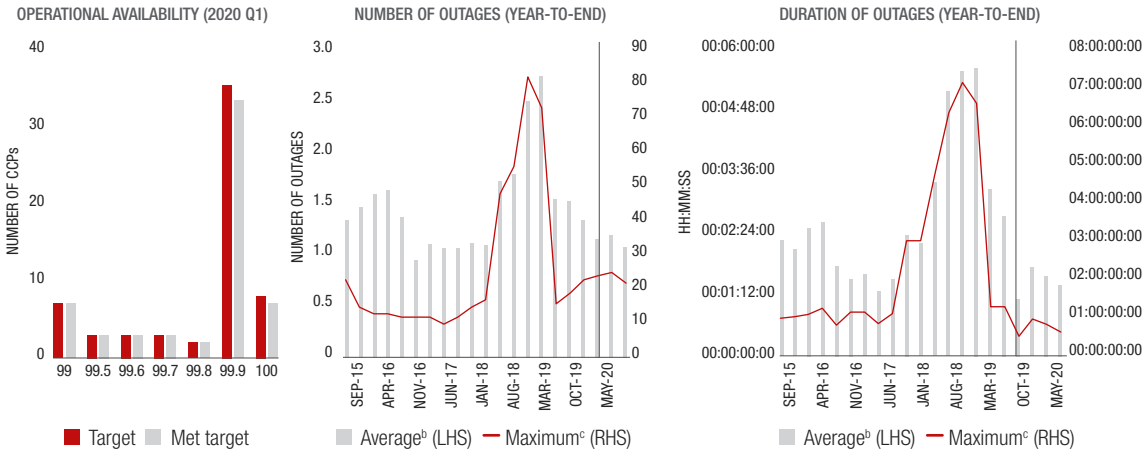
While having a backup site with a distinct risk profile is typically an effective approach for recovering from physical events such as natural disasters, terrorism, and hardware failures, it may be less effective for software issues (including recovery from a cyber attack) and pandemics. In terms of recovery from a cyber attack, the 2016 CPMI-IOSCO guidance on cyber resilience for financial market infrastructures discusses other options, such as resuming critical operations in a system that is technically different from the primary system or in a system that performs those operations and completes settlement in a non-standardized way [CPMI-IOSCO (2016)]. Financial market infrastructures' business continuity arrangements in response to the COVID-19 pandemic are discussed below.

3. CHALLENGES OF COVID-19

The COVID-19 pandemic is notable in terms of its duration and scale. The pandemic is already into the second year and is expected to persist for many more months. The near-complete shutdown in many major economies in Q2-Q3 2020 was unprecedented and led to a large drop in economic activity as well as societal adjustments. The International Monetary Fund (IMF) estimates that the global economic growth fell by 3.5 percent in 2020 as a result of COVID-related shocks [IMF (2021)]. The impact of the pandemic has also been significant in terms of labor supply, with over 2.5 million deaths worldwide [JHU&M (2021)] and scores of "recovered" COVID patients still having long-term health effects.

Financial market infrastructures have generally functioned well, despite the challenging external financial and operational conditions [FSB (2020d)]. Oliver Wyman (2020) concluded that financial market infrastructures have been robust, providing the community with stable platforms and operations, as well as timely information to transact throughout the market turmoil in early 2020. In the first quarter of 2020, when the transition to remote working was most sudden, almost all central counterparties met their operational availability target (Figure 1, left-hand panel).[8]

Figure 1: CCP operational resilience[a]



[a] Selected central counterparties (CCPs). Some CCPs report at the CCP service or system level.
[b] Average calculations include CCPs that have not reported an outage during that year.
[c] The CCP with the maximum number and maximum total duration of outages may be different and will change over time.

Source: Clarus FT, BIS calculations.

[8] Some central counterparties report at the CCP service level.

The average number and duration of outages affecting central counterparties' core systems during the COVID-19 pandemic was also largely unchanged at around one and just under one-and-a-half hours, respectively, in the twelve months ending September 2020 (Figure 1, center and right-hand panel). The average duration was largely driven by two outages that delayed client messaging processing at three central counterparties within the one group and lasted a total of almost six-and-a-half hours [DTCC (2020)].

4. BUSINESS CONTINUITY ARRANGEMENTS

As COVID-19 spread across the globe in 2020, financial market infrastructures initiated their business continuity plans. A key element was a shift from on-site to remote working. While many financial market infrastructures had remote working arrangements in place, like for other firms the scale and duration of the switch to remote working was generally unexpected. According to Oliver Wyman (2020), around 80-99 percent of IT staff and more than 50 percent of trading staff in financial services firms were working from home within two weeks of major jurisdictions enforcing lockdowns. This led to operational challenges around virtual private network and internet service provider bandwidth capacity, availability of remote infrastructure (e.g., laptops, SIM cards), and reduced productivity stemming from remote communication barriers and childcare obligations of staff. According to anecdotal evidence, even now – over a year since the start of the pandemic – financial market infrastructures in many jurisdictions have some portion of their operational staff working remotely.

Another key part of financial market infrastructures' business continuity plans for a pandemic involved their secondary sites. As noted earlier, financial market infrastructures are required to have (at least) a primary and a secondary (backup) site. Typically, there needs to be a minimum number of operational staff physically present at both sites. Consequently, it was important to have such staff recognized as essential personnel and, therefore, allowed to commute and work on site despite lockdowns [FSB (2020a)]. Having multiple sites has allowed financial market infrastructures to split their operational staff into separate teams that are physically isolated from each other to minimize the risk of one team infecting the other. Nevertheless, the widespread nature of the COVID-19 pandemic has meant that staff at both sites were often subject to the same risk. Some institutions went even further – for instance, by isolating key operational staff with strict controls on any outside contact [Roy (2020)]. Some financial market infrastructures have also identified alternative backup staff (e.g., from veterans and staff in other business areas) who could be called on in the case of severe staff shortage.

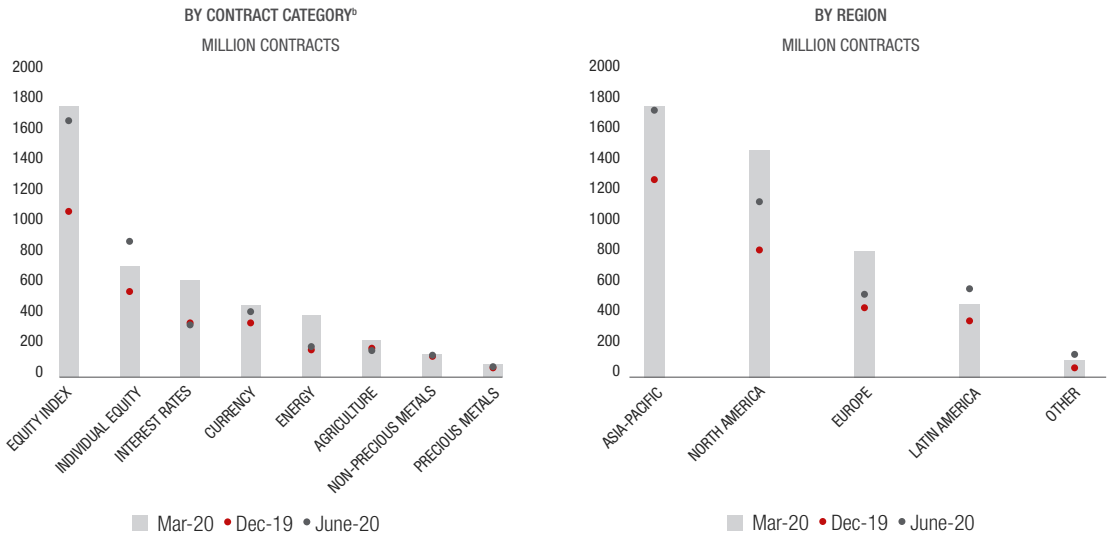
Like many firms, for the safety of essential on-site staff, financial market infrastructures have adopted a range of measures. These include enhanced hygiene on the premises (e.g., more thorough cleaning on a daily or more frequent cycle, use of special cleaning products, provision of hand sanitizers across the premises, and distribution of gloves and masks) and instituting social distancing at work (e.g., maintaining a minimum distance between desks). In addition, many entities have introduced body temperature monitoring for on-site staff.

Timely and efficient internal communication is essential for financial market infrastructures to respond quickly to any incidents (operational or otherwise) and for regular, efficient decision-making. Many financial market infrastructures have issued press releases to inform their end-users and the public of their business continuity measures and to assure stakeholders that they would continue to offer their services as normal (see Appendix for selected examples). In addition, some industry associations have also provided compilations of these initiatives in a single space.[9]

Communication between the financial market infrastructures and regulatory authorities has also increased. Generally speaking, central banks and other supervisory authorities have heightened and/or reoriented the oversight/supervision activity of their financial market infrastructures.[10] As with other financial sector authorities, the initial focus was on supporting business continuity and containing operational risk in the face of sudden and unexpected lockdowns. Financial sector authorities monitored and reviewed firms' (including financial market infrastructures) pandemic plans in light of measures taken to contain the spread of the virus. In light of remote working arrangements and possible exploitations of security weaknesses by cyber threat actors, there has also been scrutiny on cybersecurity arrangements [FSB (2020d)]. Guided by the Financial Stability Board's (FSB) principles on the public authorities' response to COVID-19, some authorities have reduced or postponed aspects of their supervisory activity (e.g., supervisory reporting, postponement of on-site visits) to temporarily reduce the operational burden on firms or authorities [FSB (2020b)].

[9] See for example https://www.iif.com/COVID-19, https://bit.ly/3cXmvkG.
[10] For example, in Hong Kong SAR, intensified supervisory monitoring of financial market infrastructures and other financial firms; see: https://bit.ly/3tQJCo0.

Figure 2: Clearing volumes[a]



[a] Worldwide data for exchange-traded derivatives given by the sum of futures and options.
[b] For the contract category "other", which is not shown in the figure, the volume of exchange-traded derivatives increased from 77.4 million contracts in December 2019 to 91.1 million contracts in March 2020 and 92.6 million contracts in June 2020.

Source: FIA Monthly Report

5. OTHER SOURCES OF STRESSES ON FMI OPERATIONS

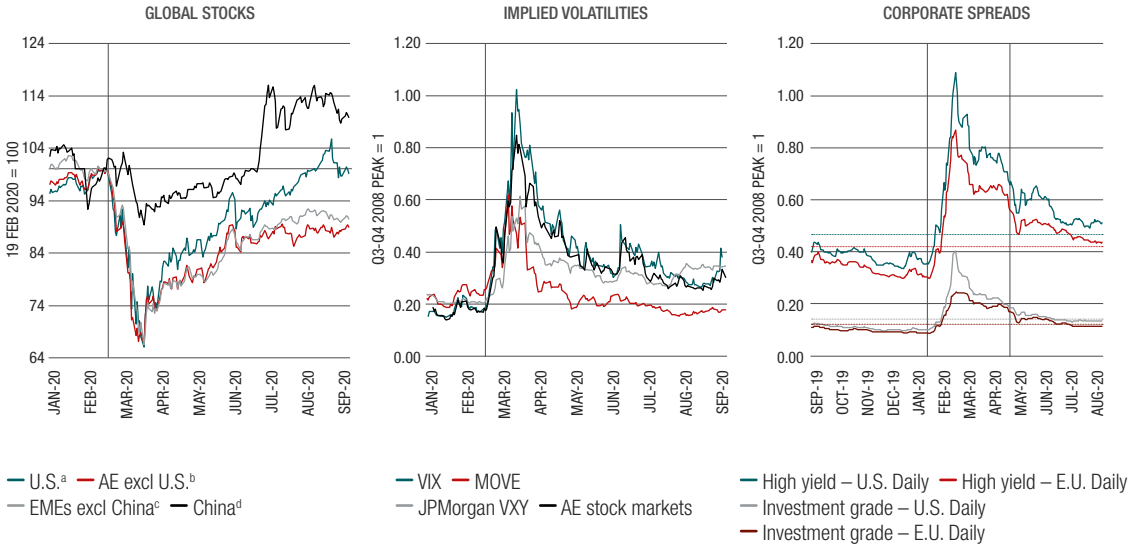
In the first few months of the global pandemic, heightened market volatility stressed payment, clearing, and settlement processes. Notably, transaction values and volumes were generally higher than normal in March and April 2020.[11] For example, the volumes of cleared transactions across almost all products and regions were elevated in the first quarter, and often remained elevated through the second quarter (Figure 2).

Increased trading volumes have led to minor operational hitches. In particular, in the initial phase there were delays in settlement of securities as market participants faced operational and other challenges in sourcing and delivering securities while most of their employees were working from home [FSB (2020e)]. According to ESMA (2020), settlement fails during the second half of March in the E.U. climbed to around 14 percent for equities and close to 6 percent for government and corporate bonds. The European Securities and Markets Authority (ESMA) attribute this to both operational issues (associated with remote working and third party outsourcing to countries in lockdown), as well as pressures from the high levels of trading activity, which led to longer settlement chains (whereby the failure to deliver a security resulted in multiple fails across the chain). Nevertheless, the ESMA found that most settlement fails were resolved between one and five days after the intended settlement date. Relatedly, some payment systems, central securities depositories, and securities settlement systems extended their operating hours on particular days in order to process the backlogs of trades.[12]

Markets were also unexpectedly volatile in March (Figure 3), which led to larger and more frequent margin calls at central counterparties [Huang and Takáts (2020), Chuang (2020), ESMA (2020)]. Central counterparties typically make daily margin calls, but when markets are volatile or positions change rapidly, they can call for additional margin intraday.[13] The unexpected volatility in March 2020 led to more frequent margin calls, which added to operational demands on central counterparties' clearing members.

[11] The change in activity in payment systems was more mixed. Payment systems that cater to retail or corporate payments sometimes reported a decrease in activity due to the downturn in economic activity due to lockdowns, while others that support online payments saw an increase in activity as purchases moved online.
[12] This was the case for the TARGET2-Securities system, which saw its daily transaction volumes double (year-on-year) in March 2020 [Panetta (2020)].
[13] For further background on margin call mechanics see Box 4.2 in FSB (2020e).

Figure 3: Volatility in March 2020 was unusual



The vertical line in left-hand and center panels indicate February 19, 2020 (S&P 500 pre-COVID-19 peak). The vertical lines in the right-hand panel indicates February 19, 2020 and May 12, 2020 (when the Fed started purchasing corporate ETFs).
The horizontal dashed lines in the right-hand panel indicate 2005–current medians.
[a] S&P 500 Index.
[b] For AEs, the series represents the weighted average of selected equity prices indexes in the following countries: AU, CA, CH, DK, Euro Area, GB, JP, NO, NZ, and SE.
[c] For EMEs, the countries are the following: BR, CL, CO, CZ, HK, HU, ID, IN, KR, MX, MY, PE, PH, PL, RU, SG, TH, TR and ZA.
[d] Shanghai composite equity index.

Sources: Bloomberg; ICE BofAML indices; national data; BIS calculations.

Almost all margin calls at central counterparties were met by the clearing members, and in the few cases where the central counterparties needed to undertake default management actions they were able to do so despite remote working arrangements. The most prominent incident involving a central counterparties was when a small futures commissions merchant (Ronin Capital), which was a member of two U.S. Central counterparties (CME and FICC), was unable to continue to meet its participation requirements due to the deterioration of its capital position. Consequently, its membership was suspended and its positions liquidated; the loss was covered by margin [CCP12 (2020)]. There were two member defaults at smaller regional central counterparties where the resulting loss exceeded margin. A member defaulted at the Polish energy central counterparty (IRGiT), which resulted in 2.07 percent of total mutualized resources being used [IRGiT (2020)]. The other incident was the default of AIK Energy Australia at Keler central counterparties in Hungary, where mutualized resources were initially used but subsequently paid back by the defaulter's estate [ISDA (2020)].

From an operational perspective, the key challenge with handling a default under remote working arrangements is managing communications with internal and external stakeholders, particularly when default management plans are based on bringing stakeholders together in physical meetings. For example, central counterparty default management plans for over-the-counter products often involve bringing seconded traders together physically to hedge and auction the defaulter's portfolio. When physical meetings are not possible, such central counterparties need to find an alternative arrangement to securely share information with seconded traders and prevent that information from being shared outside those traders.

6. ONGOING CHALLENGES

Financial market infrastructures have generally adjusted well to the COVID-19 pandemic. Nevertheless, the event has also brought to the fore a number of (known) challenges.

First, financial market infrastructures and authorities need to review, test, and update their incident management and business continuity plans to reflect the lessons learnt so far and to identify areas for enhancement in a proactive way. This may include identifying mitigating strategies for single points of failures, capacity and controls for handling manual processes, and obtaining assurance on the effectiveness of business continuity plans of third parties.

Second, financial market infrastructures will need to review the effectiveness of their control framework under current (remote work) operating arrangements. To date, financial market infrastructures have assessed, and where necessary, adapted governance arrangements to ensure that there are clear lines of communication and decision-making processes that work effectively under the largely remote operating arrangements. The effectiveness of the second and third lines of defense[14] may also be affected by the remote operating arrangements if certain activities require an on-site presence. In addition, consideration could be given to whether sufficient customer engagement can be achieved under remote operating arrangements.

Third, the pandemic has highlighted the extent of interconnectedness across economies, businesses, and financial institutions. Financial market infrastructures operate in an ecosystem with a number of other participants, and the efficiency and resilience of a financial market infrastructure are intricately linked to those of the other participants in its ecosystem. The Principles for Financial Market Infrastructures acknowledge the risks from interconnectedness with principles on "FMI links" and "access and participation requirements", guidance on external sources of operational risk including critical service providers and utilities, and an annex on "oversight expectations for critical service providers". Nevertheless, the pandemic highlighted frictions, such as:

- While financial services (including those provided by financial market infrastructures) are regarded as "essential" in most jurisdictions and thus have (at least some level of) exemption from lockdown restrictions, this may not extend to other entities that provide services to financial market infrastructures. For example, consider a situation where a financial market infrastructure relies critically on a business for some of its functions or processes (e.g., facility and IT support services) and that business is not deemed "essential".[15]
- Participants or third party service providers of a financial market infrastructure may not have as developed a business continuity plan as the financial market infrastructure itself (and vice versa). This may be especially relevant for smaller entities with (relatively) limited resources for business continuity planning. Smaller financial market infrastructures may also not have enough bargaining power vis-à-vis larger, globally active third parties to ensure the continued service provision by such third parties.
- Like other financial institutions, some financial market infrastructures experienced delays and logistical difficulties in obtaining remote working equipment from third parties due to disruptions to their global supply chains.

Fourth, cyber and endpoint security concerns have heightened. Given the scale of the remote arrangements in place, and the thereby enlarged "attack surface", the risk of cyber incidents has increased at financial market infrastructures (as well as at their participants and third parties). Notably, attackers have moved to using "COVID-19" as a subject in phishing attacks; and the higher stress levels in the workforce increase the likelihood of simple cyber attack methods being successful (e.g., someone clicking on a malicious link that highlights COVID-19 vaccines).

7. CONCLUSION

During the COVID-19 pandemic, financial market infrastructures have had to deal with major operational challenges, namely the move to business continuity operations and increased activity due to market volatility. Financial market infrastructures have generally coped well with these challenges and without major disruptions to financial activity. However, the pandemic has also highlighted some operational issues that require further consideration and improvement where needed. These include the need to review and update their incident management, risk control and governance, business continuity plans, and cyber resilience practices. It will be important for financial market infrastructures and authorities to use the COVID-19 pandemic as an opportunity to learn and further improve the resilience of financial market infrastructures and the wider financial system.

Just like real-world plumbing, if financial market infrastructures and their authorities do their job properly, general interest in how the plumbing works will fade and people will just go back to assuming that when they turn on the tap, financial assets will flow freely through the (financial market) plumbing as expected. That is how it should be.

[14] Under the three lines of defense model, the first line is risk management within the business functions themselves; the second line is an independent risk management and compliance function that develops risk management policy and oversees risk management in the first line; and the third line is independent assurance (i.e., internal and external audit).

[15] For instance, in the initial days of the lockdown in India, IT outsourcing firms – many of which provide services to financial entities in the U.S., Europe, and elsewhere – faced difficulties with their operations.

APPENDIX: SELECTED EXAMPLES OF PUBLIC STATEMENTS BY FMIS AND AUTHORITIES AT AN EARLY STAGE OF THE COVID-19 PANDEMIC

Table A: Public statements by selected FMIs/Authorities

JURISDICTION	FMI	MEASURE/MESSAGING	LINK	DATE (2020)
Australia	All	General review of impact of pandemic on Australian financial system.	https://bit.ly/3tT4t9U	April
	ASX	ASX's COVID-19 business continuity plans and activities.	https://bit.ly/2P6ceut https://bit.ly/3cgXthn	April
	RITS	Impact on operations.	https://bit.ly/3rbPB4U; Box 1	May
Canada	LVTS	Payment system continues to operate as normal.	https://bit.ly/3tQ4zPP	March 26
China	PBC[a]	Ensure continued, safe provision of banknotes and increased tolerance for reserve deposit limits.	https://bit.ly/3d5SRtf[b]	February
Hong Kong	All	Intensification of supervisory monitoring of FMIs and other financial firms.	https://bit.ly/3siDoNc	April 21
		Guidance on cybersecurity under remote office arrangements.	https://bit.ly/3d2wjtF	April 29
Indonesia	BI-RTGS	Adjustments to operational arrangements (notably operating hours) of domestic payment systems.	https://bit.ly/2Qrxpal	March 24
Japan	BOJNET	Countermeasures in response to COVID-19.	https://bit.ly/2P57Pln	May 22
Pakistan	All	Guidelines for availability and continuity of financial services.	https://bit.ly/2NLJ1nZ	March 16
		Guidelines for enhancing cyber resilience in the face of COVID-19 business continuity arrangements.	https://bit.ly/3fby4Hx	March 26
Russia	All	Extended operating hours of payment and settlements services through May public holiday period.	https://bit.ly/31k0oPP	April 29
U.S.	CHIPS	The Clearing House's response to the COVID-19 pandemic.	https://bit.ly/3ci0loU	April 23

[a] Jointly with other government and regulatory authorities. [b] Available only in Chinese. Sources: Central bank, FMI and market authority websites.

REFERENCES

BoE, 2019, "The Bank of England's supervision of financial market infrastructures – annual Report," Bank of England, February 14, https://bit.ly/31e6xNO

CCP12, 2020, "CCPs again demonstrate strong resilience in times of crisis – a CCP12 paper," July 7, https://bit.ly/39cG4nZ

Chuang, A. 2020, "Asia CCPs forced to hike margins rapidly during equities rout," Risk.net, March, https://bit.ly/397VPwE

CPMI-IOSCO, 2012, "Principles for financial market infrastructures," April, https://bit.ly/3sgLkOU

CPMI-IOSCO, 2016, "Guidance on cyber resilience for financial market infrastructures," June, https://bit.ly/3d0jUGO

DN, 2018, "Today's delay of salary and transfer income payments," Danmarks Nationalbank, press release, August 31, https://bit.ly/3chf5JP

DTCC, 2020, "CPMI-IOSCO quantitative disclosure results 2020 Q3," December 18, https://bit.ly/3977Sdh

ECB, 2020a, "Communication on TARGET incident from 23/10/2020," European Central Bank, October 25, https://bit.ly/3vV1SOM

ECB, 2020b, "ECB announces independent review of payments system outage," European Central Bank, press release, November 16, https://bit.ly/3siACaK

ESMA, 2020, "TRV: ESMA report on trends, risks and vulnerabilities," European Securities and Markets Authority, No.2, September, https://bit.ly/3tQxtza

Forbes, 2021, "Here's how scientists are using sewage water to control COVID-19," January 19, https://bit.ly/3lPG9TF

FSB, 2020a, "FSB members take action to ensure continuity of critical financial services functions," Financial Stability Board, press release, April 2, https://bit.ly/3cUDWSM

FSB, 2020b, "COVID-19 pandemic: financial stability implications and policy measure taken," Financial Stability Board, April, https://bit.ly/39aqKbC

FSB, 2020c, "Regulatory and supervisory issues relating to outsourcing and third party relationships – discussion paper," Financial Stability Board, November, https://bit.ly/3siEEzX

FSB, 2020d, "COVID-19 pandemic: financial stability impact and policy responses: report submitted to the G20," Financial Stability Board, November, https://bit.ly/2NPKwSg

FSB, 2020e, "Holistic review of the March market turmoil," Financial Stability Board, November, https://bit.ly/3rlFZoe

Huang, W., and E. Takáts, 2020, "The CCP-bank nexus in the time of COVID-19," BIS Bulletin, May, https://bit.ly/3lJO6K0

IMF, 2021, "World economic outlook update," International Monetary Fund, January, https://bit.ly/3vXv07S

IRGiT, 2020, "Utilization of the Guarantee Fund's resources to cover losses resulting from closing a clearing house member's positions," press release, April 1, https://bit.ly/3lL4ji2

ISDA, 2021, "COVID-19 and CCP risk management frameworks," International Securities and Derivatives Association, January, https://bit.ly/3d2w95B

JHU&M, 2021, "COVID-19 dashboard," Johns Hopkins University & Medicine, https://bit.ly/3cgi19G

Kiernan, P., 2021, "Fed attributes payment system outage to 'human error,'" The Wall Street Journal, February 25, https://on.wsj.com/3skwnvf

Oliver Wyman, 2020, "Financial market resilience: three waves of action for market infrastructure firms in the aftermath of COVID-19," May, https://owy.mn/3vSboC9

Panetta, F., 2020, "Beyond monetary policy – protecting the continuity and safety of payments during the coronavirus crisis," ECB Blog Post, https://bit.ly/3rlH7Z0

RBA, 2019, "Assessment of the Reserve Bank information and transfer system," Reserve Bank of Australia, May, https://bit.ly/3d5YW9i

Reuters, 2020, "CREST problems return, Bank of England delays gilt buy-back," September 14, https://reut.rs/31dw4qe

Roy, A., 2020, "RBI's coronavirus contingency plan: keep it going from a secret location," Business Standard, March 21, https://bit.ly/3vWsxuE

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO