

**Sarah Breeden**

Executive Director

Financial Stability, Strategy and Risk

**Duncan Mackinnon**

Executive Director

Supervisory Risk Specialists

29 March 2023

Dear SMF 24 or equivalent,

## Thematic findings from the 2022 cyber stress test

We are writing to share the thematic findings from the Bank of England's cyber stress test (CST22). The findings support individual and collective work to improve the financial sector's response to and recovery from incidents.

These findings are relevant to PRA-regulated firms and financial market infrastructure firms (FMIIs), including firms that did not participate in the test. Therefore, we strongly urge all such firms to reflect on these findings and incorporate relevant aspects in their continuing implementation of operational resilience and related policies.

We would like to thank the firms that participated in the cyber stress test for their constructive engagement.

## Background and context of the Test

In June 2017, the Financial Policy Committee (FPC) set out its framework of regulation for the UK financial system's cyber resilience to mitigate systemic risk, which included regular testing of firms' resilience by firms and supervisors.<sup>1</sup> In March 2021, the FPC

---

<sup>1</sup> <https://www.bankofengland.co.uk/financial-stability-report/2017/june-2017>.



set its impact tolerance – that the financial system should be able to make payments on the date they are due (ie by the end of the 'value date').<sup>2</sup>

The FPC also acknowledged that there might be instances where the disruption caused by an incident was such that, despite prior planning, attempting to recover by the end of the value date could have a more adverse impact on financial stability than failing to do so, and findings from the 2022 cyber stress test reinforced this view. The test also indicated that there might be scenarios where it was not possible for firms to restore their services before recovery of a third-party (eg where a financial market infrastructure was disrupted). Therefore, the FPC impact tolerance has been updated to factor in both these situations. Please see the March 2023 FPC Record<sup>3</sup> for further details.

Regular cyber stress tests are intended to test firms' ability to meet impact tolerance in severe, but plausible scenarios. Firms are invited to participate based on the significance of their contribution to the operations of the UK financial system's vital functions.

As set out in the March 2021 FPC record, the objectives of CST22 were to explore:

- firms' ability to quickly identify the nature of the disruption they faced; and
- the potential financial stability impacts of firms not meeting the impact tolerance in the case where data integrity had been compromised.

In December 2021,<sup>4</sup> the PRA announced its plans to invite a number of systemic, as well as smaller firms, to participate in a voluntary cyber stress test which would focus on a severe but plausible data integrity scenario on a retail payment system. Cyber stress testing is a relatively new tool, and in view of this, the FPC agreed that the 2022 test would be an exploratory test, rather than a formal pass-fail assessment, and was conducted as a desktop exercise. Participating firms would; however, be expected to share their findings with supervisors.

## Scenario

The test was based on a hypothetical data integrity scenario affecting retail payments. A threat actor, aided by a malicious insider, sought to redirect payments by amending payee data concurrently at two distinct firms. The hypothetical attack was detected and confirmed out of business hours. In line with the operational resilience policy, the test

---

<sup>2</sup> <https://www.bankofengland.co.uk/financial-policy-summary-and-record/2021/march-2021>

<sup>3</sup> <https://www.bankofengland.co.uk/financial-policy-summary-and-record/2023/march-2023>.

<sup>4</sup> <https://www.bankofengland.co.uk/prudential-regulation/publication/2021/december/cyber-stress-test-2022-retail-payment-system>

assumed that disruption had occurred and did not examine preventative or detective controls.

The scenario used was hypothetical and designed to explore firms' response and recovery options. It was not based on any information on threat intelligence or vulnerabilities in the system.

Subject to maintaining the scenario's severity, test participants were given the flexibility to adapt the scenario to their own business models and technical systems.

## Key Findings

### Industry coordination

Timely and co-ordinated decision-making and action across the industry is critical in limiting the impact of an incident. Consistent with the Bank and the PRA's policies, and the FPC's impact tolerance, firms should make decisions taking into account the potential consequences of their actions on others, and understand the actions that others might take to contain the risk of contagion. To support this, it is essential that response actions, including any potential rerouting of payments via alternative payment systems, and public communications are co-ordinated effectively across the industry. The existing Sector Response Framework<sup>5</sup> plays an important role in this co-ordination.

We encourage the sector to leverage existing fora to develop principles-based playbooks to help industry understand how others are likely to act in this kind of scenario and to define delegated decision-making where relevant cross-industry fora might be unable to decide quickly enough. FMIs have their own fora to co-ordinate with participants in their systems and should make use of those networks and the Cross-Market Operational Resilience Group (CMORG) also plays an important role in this space.<sup>6</sup> We also encourage firms to review how decision-making and co-ordinated action across the sector is best executed out of business hours in cases when prompt action is needed to contain an incident. The Bank and PRA will follow developments in this area closely.

---

<sup>5</sup> <https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector>.

<sup>6</sup> Please see: <https://uk.linkedin.com/company/cmorg>. This should build on work the industry have already done to develop a System Integrity Reconnection Framework to support after technical quarantine in a cyber incident and their work on GBP Payments Prioritisation Framework to define critical payments.

---

## Communication

Consistent, effective, and timely communications are important throughout an incident. Firms must communicate with a wide range of stakeholders internally and externally, including, for example, customers, the public, regulators, the media, and other participants in the payments system. This communication occurs across a number of channels, including via the Sector Response Framework, social media channels, and traditional media. Aligning communication across entities and through channels is an important tool for maintaining public confidence in times of extreme stress.

Given the short amount of time for responding to an incident, it is important for firms to consider how pre-scripted messages, which can be adapted to the specifics of the incident, could help maintain public confidence. Such pre-scripted messages should be considered for both individual firms and across the industry collectively.

## Contingencies

Rerouting payments via alternative payment systems, where possible, could help to lessen the impact of an incident. Therefore, it is crucial that firms test payment rerouting processes to operate safely, quickly, and at scale.

It is important for firms to explore what contingencies are already available to them and consider how different contingencies could work together in an incident. Further work may be needed to develop options for responding to an incident, by improving existing contingencies and/or developing and investing in new ones. It is important for firms to consider the capacity in the fall-back systems in contingency options they intend to rely on.

We also urge firms to identify and prioritise critical payments which will aid firms' focus on payments that are the most important for managing the impact on financial stability.

## Mitigants

Suitable mitigating actions, such as providing emergency cash or extending overdrafts in the case of retail payments, could help to maintain public confidence in the financial system and therefore limit the risk of an incident causing financial instability. Therefore, it is crucial that robust and scalable processes exist which allow firms to mitigate the impact of failing to make payments by their value date. It is important for firms to consider what mitigants might be suitable to their businesses, develop and invest in them as necessary, and ensure processes to action those mitigants are both robust and scalable.

Development of sector-wide frameworks to standardise how mitigants, such as the distribution of short-term credit or emergency cash, are applied, would be beneficial to minimise confusion for consumers.

## Reconciliation

The availability of clean data that can be used to reroute accurate payments via contingency systems and to restore a service after a data integrity incident is an important step in being able to recover payment systems. Therefore, it is important for firms to develop and test suitable tools and/or scripts to help automate data reconciliation in advance of an incident.

FMI's are likely to be key providers of clean data during data integrity incidents. As a result, FMI's should plan to meet that need in advance of such an incident and prepare and test processes to do so. Equally, firms having a direct dependency on FMI's should plan, prepare, and test processes to receive this clean data, as well as explore the availability of alternative reliable data sources.

## Testing capabilities

It is important that firms undertake appropriate planning, preparation, and testing to further strengthen individual firm capabilities and the underpinning assets, including technologies and processes which support the industry's ability to respond and recover. It is important for firms to review their testing plans to ensure they cover a broad range of scenarios across confidentiality, data integrity and availability.

## Next Steps

The Bank's continuing focus on operational resilience was reiterated in the 2023 priorities letters to PRA-regulated UK deposit takers<sup>7</sup> and international banks,<sup>8</sup> and in the Supervision of FMI's Annual Report 2022.<sup>9</sup> PRA and FCA-regulated firms and FMI's are expected to have identified and mapped their important business services, set impact tolerances for these and commenced a programme for scenario testing. The Bank has previously communicated<sup>10</sup> that the cyber stress test is a separate but complementary exercise to operational resilience policy. However, we expect that firms will draw on the test's key findings, as laid out in this letter, and incorporate relevant

---

<sup>7</sup> <https://www.bankofengland.co.uk/prudential-regulation/letter/2023/uk-deposit-takers-2023-priorities>.

<sup>8</sup> <https://www.bankofengland.co.uk/prudential-regulation/letter/2023/artis-2023-priorities>.

<sup>9</sup> <https://www.bankofengland.co.uk/news/2022/december/supervision-of-financial-market-infrastructures-annual-report-2022>.

<sup>10</sup> <https://www.bankofengland.co.uk/prudential-regulation/publication/2021/december/cyber-stress-test-2022-retail-payment-system>.

test findings to ensure that their important business services can remain within impact tolerances in severe, but plausible scenarios, by March 2025.

The Bank and PRA will be proactive in the monitoring of firms' implementation of the operational resilience policy ensuring that firms are ready to remain within their impact tolerance as soon as possible and no later than March 2025. Firms will be expected to show that they are testing against severe but plausible scenarios, such as the one used in the 2022 cyber stress test, and this testing should become more sophisticated over time. Firms are expected to demonstrate through testing, that they are able to remain within impact tolerance or, when they are unable to do so, to invest and take action to improve their operational resilience.

A key outcome sought by the Bank is that firms embed the policy expectations to take action to improve their operational resilience. This means firms are expected to have assessed their risks, vulnerabilities, and dependencies, and where these may threaten their ability to remain within impact tolerances through severe, but plausible scenarios, the firm should have a plan to remediate them. Firms should share with their supervisors how they have assured themselves that their investment plans deliver the necessary improvements. The Bank and PRA expect to see the testing and remediation workplan that provides board-level assurance that the firm will be able to remain within impact tolerances. These should be included in firms' self-assessments.

Firms may need to take forward the lessons from these findings at firm, FMI, and/or sector level as appropriate, to further enhance the sector's resilience and the Bank and PRA would expect these findings to build on work that is already underway, including sector-wide frameworks that have been developed.

The results of this test have highlighted the importance of firms planning, preparing, and testing for such situations alongside investment so that the impact on financial stability and any other secondary impacts are minimised. It is important that firms invest in areas which would enhance their capability to respond to and recover from incidents. Investment in suitable mitigants may also be necessary to better manage risks to financial stability during an incident. The Bank will also consider how best to monitor and gain assurance over firms' work on these capability enhancements.

In addition, the Bank and PRA are challenging firms in areas where they need to work across the sector to respond to different scenarios, such as this one. The Bank, PRA and FCA are closely involved in the work of CMORG and will continue to work with them as partners on this.

The Bank and the PRA will consider the learnings from this test to inform future work in this space.

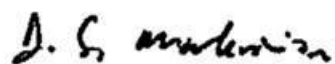
Yours faithfully

A handwritten signature in black ink that reads "Sarah Breeden". The signature is written in a cursive style with a long horizontal flourish at the end.

**Sarah Breeden**

Executive Director

Financial Stability Strategy and Risk

A handwritten signature in black ink that reads "D. S. Mackinnon". The signature is written in a cursive style with a long horizontal flourish at the end.

**Duncan Mackinnon**

Executive Director

Supervisory Risk Specialists