



BANK OF ENGLAND

Speech

Enhancing resilience in payments

Speech given by

Victoria Cleland, Executive Director; Banking, Payments & Innovation

PayExpo, London

8 October 2019

With thanks to Samantha Leighton and James Sanders for their assistance in preparing this speech.

It is a pleasure to be speaking at PayExpo at the Business Design Centre in Islington today, in an agenda packed with innovation and technological advance. I lived in Islington when I first moved to London, which had the great benefit of enabling me to walk to work. I now live further afield, but I am able to make the journey in similar time benefitting from advancements in new(er) technology – a bicycle!

It is also a pleasure to be speaking at a second major payments event in London in a month, following hot on the heels of SIBOS in late September. This demonstrates the importance of London, and the UK, as a hub for payment innovation and fintech more widely. In the second quarter of 2019 funding for fintech companies topped \$8.3bn, growing 24% quarter-on-quarter¹ – just one sign of a thriving industry. The number of payments made in the UK continues to increase too and reached a record 39 billion in 2018, with a value of more than £90 trillion.² We are also experiencing a period of rapid change in the way payments are being made (one can even hire an electric bike using an app) by consumers and businesses, and in the companies and technologies behind them.

At SIBOS I spoke³ about the Bank of England's engagement with innovation and future trends in payments, both through our response to the Future of Finance Report⁴ and our work to renew the UK's Real-Time Gross Settlement (RTGS) service. This is an ambitious programme which will be delivered over the next few years. Our vision for RTGS is defined by: increased resilience; greater access; wider interoperability; improved user functionality; and strengthened end to end risk management. Today I will focus on the steps we are taking right now on the fifth of these to enhance the resilience in payments.

Operational risk and resilience are in the spotlight like never before, with the FCA reporting a 187% increase in technology outages from 2017 to 2018.⁵ The joint Discussion Paper the Bank, PRA and FCA published last year⁶ started a dialogue on the operational resilience of the financial system, and the individual firms and Financial Market Infrastructures within it. I will discuss resilience through a payments lens.

The UK's payment systems (including retail payment systems such as Faster Payments and Bacs, and the high value system – CHAPS) connect payment service providers (PSPs) together, as a means of moving money between them. It is therefore vital that the organisations that manage the payment systems dedicate a lot of time to enhancing operational resilience and cyber security. And innovations, including instant payments, will also benefit from a resilient foundation.

The Bank's operation of RTGS, and more recently CHAPS, makes a vital contribution to our overarching mission of maintaining monetary and financial stability. CHAPS is the UK's high value payment system and settles an average of £330 billion each working day, representing 93% of non-cash payments in the UK by

¹ <https://www.assetnews.com/fintech/europe-trumps-asia-fintech-funding-q2-2019>

² <https://www.ukfinance.org.uk/sites/default/files/uploads/pdf/UK-Finance-UK-Payment-Markets-Report-2019-SUMMARY.pdf>

³ <https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/payments-a-platform-for-innovation-speech-by-victoria-cleland.pdf?ja=en&hash=5841227A82F5C75B75FFE32027EEF5EDA61D2C70>

⁴ <https://www.bankofengland.co.uk/report/2019/future-of-finance>

⁵ <https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf>

⁶ <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf>

value. RTGS is the infrastructure where the key UK payments systems – including CHAPS – ultimately settle, supporting stability across the broader financial system.

The area of the Bank that I lead (Banking, Payments and Innovation) has provided real-time settlement through our RTGS infrastructure since 1996. In 2017, as part of our vision to enhance stability, we took the step of bringing the management and operation of CHAPS into the Bank (until then the CHAPS payment scheme was operated by a private sector company – CHAPS Co). The Bank understood and mitigated the risks within RTGS, and CHAPS Co looked at risks in its participants. But it was hard to join the two views together. Bringing CHAPS into the Bank meant a single organisation could take a holistic approach to managing risk across the end-to-end CHAPS system.

It also meant we could draw on a wide range of skills within the Bank – from supervision to cyber. This change enabled the teams responsible for operation of CHAPS to work closely with colleagues in the PRA, who are responsible for supervising most of our participants, and to access a range of information and tools to effectively challenge risk management practices in our users. Another area of the Bank, responsible to a different Deputy Governor, continues to supervise CHAPS to the same standards as other systemically important FMIs.

As a single unified operator for CHAPS, as well as RTGS, the Bank is taking important steps as a standard setter and a thought leader to drive increased resilience and improved recovery capability in payments.

Minimising risk

Standards

As the operator of CHAPS, the Bank is well placed to drive greater resilience in members of CHAPS through the setting of standards. This is complemented by the Bank's role as prudential regulator of many of these firms.

In order to manage risk, a payment system has rules to govern who can join, how participants should behave, and what operational and technical requirements they must meet. The CHAPS Reference Manual (CRM)⁷ contains the rules and requirements that CHAPS Direct Participants must comply with. The bulk of the requirements effectively describe controls that each Direct Participant must have in place – and these controls collectively are designed to mitigate the key risks to the end-to-end CHAPS system and support financial and operational resilience.

Importantly, this includes risks the participants pose to each other. For example, the 'Throughput' rules require direct participants to process a certain proportion of payments by value by fixed times in the day. By

⁷ <https://www.bankofengland.co.uk/-/media/boe/files/payments/chaps/chaps-reference-manual>

smoothing the flow of payments across the operating day rather being concentrated at stress points such as the end of day, this approach contributes to both financial and operational resilience.

We require participants to attest to meeting the CRM requirements and we also undertake verification. But risks to the payment system are constantly changing and we need to ensure that the CRM adapts accordingly. Outages of CHAPS may disrupt the smooth flow of critical and time-sensitive payments that are core to the smooth operation of the financial system and real economy. Such outages would hurt end users and, if frequent and prolonged, potentially undermine monetary and financial stability. We are currently working on three sets of requirements to further mitigate these risks: cyber, incident management and Cloud.

First, we plan next year to enhance the Security Requirements in the CRM to align to the globally recognised National Institute of Standards and Technology (NIST) Cybersecurity Framework.⁸ The new requirements would align with NIST's principles of Identify, Protect, Detect, Respond and Recover, and will be more outcome focused, balanced with prescriptive requirements when necessary. This will increasingly enable Direct Participants with different resources and business models to apply their own methodology to comply, thus supporting our strategy to allow a diverse range of financial institutions to use CHAPS.

Second, the CHAPS rulebook clearly defines the Bank's expectations around Direct Participants' incident management approaches and reporting obligations. As I mentioned earlier, the FCA has observed a significant increase in technology-related outages across the financial industry. And for the first eight months of 2019, there were around half a dozen CHAPS Direct Participant incidents a month. The CHAPS rulebook provides an effective and timely means to manage risks through a focused root cause analysis, assignment of appropriate remediation plans and trend analysis to inform our assessment of the risks to the end-to-end CHAPS system. In line with the FCA's analysis of incident reports,⁹ we have found that weaknesses in how changes are managed is a key driver behind nearly half of all CHAPS participant incidents. We are therefore revising the controls that Direct Participants should have in place in order to target areas that have contributed to incidents, for example, single-input of static data.

Third, in a payments industry that is experiencing a period of rapid change in technology, Cloud technologies are growing in importance. The Bank is taking steps to facilitate its adoption, including issuing a supervisory statement later this year. The use of a Cloud model is an evolution of, and a key element in, the supply chain for many financial institutions – including those who access CHAPS. We believe the use of Cloud technologies has the potential, if used appropriately, to minimise end-to-end risk and improve operational resiliency of the CHAPS system, taken as a whole. As the operator of CHAPS we want to enable our current and potential Direct Participant to realise these benefits in a safe and controlled way, without compromising the resilience of the CHAPS ecosystem. We are assessing the risks that the use of Cloud technology

⁸ <https://www.nist.gov/cyberframework>

⁹ <https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf>

presents to the CHAPS system, and the nature of mitigating controls that we require. In due course, we expect to propose new controls for Cloud usage as it relates to CHAPS.

Policy Development

Development and implementation of requirements must be supported by strong and innovative policy thinking. The Bank works collaboratively on policy with other FMIs and central banks internationally. Some work-streams focus on resilience, others support greater innovation: and increasingly we look to combine the two.

CHAPS has historically had a small number of Direct Participants and a much larger number of indirect participants which access the system through a sponsor bank. This arrangement (known as ‘tiering’) introduces credit, liquidity and operational risks, which were brought into sharp focus by developments including the financial crisis. With heavy tiering, if a large direct participant was to encounter financial or operational issues, this would also impact the ability of the indirect participants that rely on it to make payments – causing issues to spread further across the financial system. These risks are best addressed by increasing direct access to the CHAPS system to reduce concentration in a small number of large sponsor banks.

As a result, the Bank has worked for several years, initially with CHAPS Co and more recently as the operator of CHAPS, to implement a strategy to mitigate the risks arising from tiering in CHAPS. This includes engagement with large indirect participants, as well as new CHAPS rules that presume organisations responsible for more than 2% of CHAPS value will join directly. The last decade has seen a significant reduction in financial risks associated with tiering, with the addition of a further 19 Direct Participants including two further FMIs. Despite this, CHAPS remains highly tiered relative to other high value payment systems such as Fedwire Funds and TARGET2. The renewed RTGS service will help to change this. It will be able to support several hundred direct participants and make it easier, quicker and cheaper to join CHAPS. In time, we will consider the case for reducing the 2% threshold to further enhance financial stability.

Payments fraud and economic crime are becoming increasingly sophisticated, and the Bank as operator of CHAPS is engaging in initiatives to tackle these threats. The Committee on Payments and Market Infrastructures (CPMI) has developed guidance on reducing the risk of wholesale payments fraud related to endpoint security.¹⁰ The Bank is currently undertaking a number of initiatives to strengthen our position and support our CHAPS Direct Participants in line with CPMI strategy, which includes adjusting our CHAPS rulebook to focus on detection, prevention and response to security issues as I described earlier.

¹⁰ <https://www.bis.org/cpmi/publ/d178.htm>

At the level where fraud is most likely to touch on end-users, Vocalink piloted an anti-money laundering tool known as Mule Insights Tactical Solution (MITS)¹¹ for a number of Faster Payments participants. MITS can retrospectively track fraudulent payments as they move between customer accounts, thereby helping to quickly identify and highlight to Payment Service Providers any suspected 'mule accounts'. They can then take action to block funds and close these accounts, making it more difficult for fraudsters to undertake scams. We are currently in the exploratory phase of a pilot to use MITS on a subset of CHAPS data. The additional insights generated should help participating Direct Participants to better tackle further fraud activity.

We are also focused on how as operator of CHAPS the Bank can support UK-wide efforts to tackle economic crime. The recently published UK Economic Crime Plan¹² noted the role that the Bank can play in this regard, including by enabling enhanced payment data through the development of interoperable message standards and by promoting wider adoption of Legal Entity Identifiers. These initiatives will help to promote greater transparency in ownership of legal entities and support detection of financial crime.

Minimising impact of incidents

Resilience is key to payments, and we need to be ready to respond to the unexpected. That is why we have not stopped at prevention. We are also proactively thinking about how to respond when incidents occur; how to reduce the impact and any spill-overs to the wider ecosystem; and of course how we can recover quickly (for FMIs this means within two hours under most scenarios as set out in CPMI guidance). Furthermore, like other systemically important systems, we are preparing to meet the Bank's forthcoming operational resilience policy that will apply equally to the Bank as the operator of CHAPS as it does to payment systems recognised for statutory supervision.

Our mandate for promoting the stability of the UK's financial system means we are not only interested in the resilience of CHAPS, but also the settlement of all payments critical to the economy. In an increasingly fast-moving financial system, being able to guarantee that critical payments settle on the same day is crucial. The Bank's Financial Policy Committee set out a pilot impact tolerance in March 2019¹³, stating that it would be prudent to expect the financial system to complete all critical payments by the end of the day, but recognising that firms would not be able to meet this in the most extreme circumstances. The Committee, which is responsible for monitoring and reducing systemic risks for the UK's financial system, also agreed a pilot stress test based on the temporary unavailability of payments infrastructure.¹⁴ As the operator of CHAPS, we are participating in the pilot, any lessons learned from which will further enhance our understanding of the end-to-end resilience of the CHAPS system.

¹¹ <https://connect.vocalink.com/2018/december/mits/>

¹² https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816215/2019-22_Economic_Crime_Plan.pdf

¹³ <https://www.bankofengland.co.uk/-/media/boe/files/financial-policy-summary-and-record/2019/march-2019.pdf>

¹⁴ <https://www.bankofengland.co.uk/-/media/boe/files/financial-policy-summary-and-record/2019/march-2019.pdf>

We are also working through an enhanced programme of regular testing for our tertiary solution – MIRS, the Market Infrastructure Resiliency Service which is a geographically-remote and technologically diverse solution provided by SWIFT. MIRS is designed to, within a small number of hours, pick up CHAPS payment processing and other RTGS settlements in the event of a major issue with our own RTGS infrastructure. This should mean that all critical CHAPS payments are completed by the end of the value date in line with the FPC's pilot impact tolerance. The testing programme is not just technical but ensures sufficient familiarity across staff within the CHAPS participants of the tertiary service.

We actively support the design of, and participate in, a number of market wide exercises to explore coordination in the unlikely event of a major outage to the retail systems, or participants' connections to the retail systems. SIMEX16 focused on a multi-day outage to RTGS and SIMEX18 focused on a protracted operational outage of a Global Systemically Important Bank; a summary report of SIMEX18 was published last month.¹⁵ Next month, we will participate in a desktop exercise to explore the impact of large scale re-routing of payments between CHAPS and Faster Payments. These exercises are sponsored by a Cross Market Operational Resilience Group which is co-chaired by UK Finance and the PRA.

The Bank and Pay.UK are also exploring a potential solution for allowing batches of critical retail payments to settle directly over the renewed RTGS infrastructure, whilst ensuring critical wholesale payments are not impacted. This solution could help the FPC's pilot impact tolerance be met for retail payments in the unlikely event of a major outage to the retail systems. Providing additional channels for retail payments to settle in a contingency situation increases the resiliency of the whole financial system, making it even less likely that users will experience a delay to their salaries, pensions, or other time sensitive payments.

The Bank is planning to introduce ISO 20022, an international standard for financial messaging, for CHAPS. Pay.UK also plan to introduce ISO 20022 in their New Payments Architecture: together we are developing what is known as a Common Credit Message. For the first time, the UK's primary payment systems – CHAPS, Faster Payments and Bacs – will be using the same messaging standard. This will be a major step towards interoperability of the UK payment systems and should facilitate improved contingency arrangements for critical and time sensitive payments as described above. And ISO20022 messages will contain richer data in payments, ensuring that PSPs can easily identify and prioritise the most critical payments for processing during contingency scenarios.

In the last few days we have received the industry feedback on our like-for-like schemas for CHAPS, the final version of which will be published in December alongside more information on our transition approach. The schema for the enhanced messages will be published towards the end of 2020, aiming to cut over to the ISO messages in the first half of 2022.

Conclusion

¹⁵ <https://www.bankofengland.co.uk/report/2019/sector-simulation-exercise-simex-2018-report>

There is a significant amount of work underway to ensure the continued resilience of the UK's payments infrastructure. And this work must continue, both practical activities such as testing, and also the development and promotion of standards.

Given the network nature of payments, this is not something the Bank of England can undertake in isolation. It is a journey we are on with many of you here today – the financial institutions that use CHAPS and RTGS to provide critical payment services to customers. And we continue to work closely with other FMIs such as SWIFT, Pay.UK and payment system operators in other countries to develop consistent approaches and solutions.

To ensure resilience is maintained end-to-end, payment system participants, operators and suppliers will need to continue to evolve their resiliency arrangements and cyber security protocols. While some changes can be delivered by organisations in isolation, many require the industry to work together to improve the overall level of resilience, and ultimately stability.