



BANK OF ENGLAND

Speech

The Financial “Plumbing” Committee: from Plumbing to Policy

Speech given by

Elisabeth Stheeman, External Member of the Financial Policy Committee

Institute of Directors and Burness Paull, Virtual Event

9 September 2020

I am grateful to Grainne McGread for her assistance in drafting these remarks and Mehregan Ameri (FCA), Farid Anvari, Ellen Caswell, Matthew Corder, Ronnie Driver, Jas Ellis, Lee Foulger, Renee Horrell, Wai Keong Lock, Priya Mistry, Lyndon Nelson, Josh Sadler, Jonathan Sepanski, Richard Spooner, Nick Strange, and John Sutherland for their input, as well as my colleagues on the Financial Policy Committee including the Governor, Deputy Governor for Financial Stability, Charles Roxburgh (HMT), Anil Kashyap, and former Committee Member Martin Taylor.

Introduction

Over the past few months we have all had the experience of essential things we once took for granted suddenly disappearing. Whether it was our freedom to go outside, to see friends and family, or even to get a haircut, we can all now identify with the old saying, ‘you don’t know what you’ve got until it’s gone’.

For the financial system, a striking demonstration of this was the 2008 global financial crisis. At the height of the crisis the provision of essential financial services came under threat. I remember, for example, the queues outside Northern Rock as customers were faced with losing money from their cash savings, until the government expanded its safety net for deposits.

The infrastructure – or, as I like to call it, “the plumbing” – that provides vital services is largely invisible to us until it no longer works. In the 2008 financial crisis it was only when the pipes of global finance were under threat and financial stability at risk that market participants, policymakers, and the public realised how vital it was, and to never take it for granted.

The Financial Policy Committee, known as the FPC, was formed around a decade ago because of this realisation. The Committee is normally made up of thirteen members, six of which are Bank of England staff, including the Governor as chair. The Committee also includes the Chief Executive of the Financial Conduct Authority and one non-voting member from HM Treasury. I am one of five external members of this Committee. External members are selected from outside the Bank for our experience and expertise in financial services.

Pre-crisis, no single authority had the mandate or tools to look after the stability of the financial system as a whole. Now it is the job of the FPC to take the systemic view in order to ensure the consistent supply of the financial system’s vital services. Put another way: one of the jobs of the FPC is to ensure that the basic financial plumbing works even when conditions get difficult. This financial plumbing is the infrastructure that allows transactions to be completed, such as payment, settlement and clearing providers.

We have a mantra that underpins everything we do as a Committee. This mantra is: “that it is the role of the FPC to ensure that the UK financial system is prepared for, and resilient to, the wide range of risks it could face. This is so that the financial system can serve UK households and businesses in bad times, as well as good.”

Since the financial crisis the FPC has worked to improve the resilience of the financial system, for example by increasing capital levels for banks, as you can see in Figure 1, and introducing Recommendations for mortgage lending. The covid shock has been a test of this resilience, one that the financial plumbing has so far passed. But there is no room for complacency: firms had time to prepare for covid, it evolved slowly at first, allowing them time to adapt. Furthermore, it was symmetric in nature, so all firms were in the same

position. Covid is a stark reminder that there are many types of risks that could affect the provision of vital financial services.

The FPC has always recognised this.

The former Bank of England Governor and previous Chair of the FPC, Mark Carney, noted in a 2018 speech that, “While past crises had their roots in financial losses, in our digital era systemic shocks can also come from non-financial sources.”¹ And a fellow member of the FPC, Deputy Governor for Financial Stability, Sir Jon Cunliffe, has emphasised that, “All types of financial market infrastructure firms face operational risks. Indeed, for many of these firms, it is the ‘number one’ risk they face. A serious operational incident affecting one of these global pipes is likely to have an impact on the system as a whole in several jurisdictions, rather than just upon the infrastructure firm itself.”²

Today I’d like to focus on these operational risks and speak about how the FPC will continue to build up the operational resilience of the financial system.

Building the operational resilience of individual firms

Operational risk is the risk of disruption from systems and processes, from human errors and management failures and from external events and external actors. Good operational risk management helps a firm to prevent and protect against disruption. Operational resilience on the other hand, is the ability of firms and the system as a whole to prevent, respond to, recover and learn from operational disruptions. Therefore, if operational risk is managed effectively, it will reduce the number of instances a disruption will occur.

Managing operational risk and building operational resilience may sound like common sense, particularly in light of the covid shock. However, the collective nature of the challenge means it is not always given proper priority on board agendas.

In addition to my role as an External Member of the FPC, I am also an external member of the Bank of England’s Financial Market Infrastructure (FMI) Board. In this capacity I oversee the supervision of individual financial market infrastructure firms, such as payment systems, like the firm LINK which supports the ATM service when you withdraw cash. The FMI Board also oversees central counterparties such as ICE and LCH. In this role I see first-hand how building operational resilience is a challenging prospect for many firms.

Why is this the case? It is partly because operational risk is challenging to define and measure. Before one of the key pieces of international banking regulation, known as Basel II, was written in the late nineteen

¹ ‘New Economy, New Finance’, Mansion House Speech (Carney 2019)

<https://www.bankofengland.co.uk/speech/2019/mark-carney-speech-at-the-mansion-house-bankers-and-merchants-dinner>

² ‘Global Pipes’, Speech (Cunliffe 2017)

<https://www.bankofengland.co.uk/speech/2017/global-pipes-challenges-for-systemic-financial-infrastructure>

nineties, “operational risk was largely a residual category for risks and uncertainties which were difficult to quantify, insure, and manage in traditional ways”.³ Even with Basel II, the focus was on building capital, which can provide **financial** resilience, but we also need to look at **operational** resilience. Since then many approaches to quantify and manage operational risk have been developed, but the fundamental challenges remain. For instance, many operational risks are low probability, high impact events that are inherently difficult to predict and costly to protect against. Cyber risk is the most well-known example.

If operational **risk** itself is difficult to predict and measure, how can firms know what level of operational **resilience** is enough? It is a difficult task to ask of each individual firm alone.

This is where regulatory authorities can help. In the UK the financial regulators are made up of the Bank of England, the Prudential Regulation Authority (PRA), and the Financial Conduct Authority (FCA). These authorities have made strides in setting out an approach to operational resilience in two papers published in 2018 and 2019.⁴ These papers help define the problem and set out proposals for improving operational resilience in order to protect the wider financial sector and the UK economy.

The regulatory authorities are clear that operational resilience is not just about prevention. It is also about cure. Firms should start from the premise that an operational incident **will occur** and cause disruption to vital services. **It is not a question of if, but when**. Regulatory authorities expect that firms should have robust and reliable arrangements in place to deal with this inevitable disruption.

In addition to this, as we saw during the financial crisis, accounting for the disruption experienced by individual firms is not enough to prevent a threat to wider financial stability and therefore disruption of the financial “pipes” that serve the real economy.

Therefore, the consultation papers emphasise that it is also critical to think about how firms are interconnected, and where there may be dependencies between firms. We must build the operational resilience of the whole financial system, not just individual firms and the services they provide. This is the role of the FPC, as illustrated in Figure 2 on the slide.

The FPC has identified two priority areas to promote systemic operational resilience: cyber and payments. I will now speak to both of these in turn.

³ Michael Power (2003), ‘The invention of operational risk’, ESRC Centre for Analysis of Risk and Regulation <http://eprints.lse.ac.uk/21368/1/DP16.pdf>

⁴ (2018) Discussion Paper, ‘Building the UK Financial Sector’s Operational Resilience’, and (2019) Consultation Paper, ‘Building operational resilience Impact tolerances for important business services’ <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper>

Cyber risk

One of the most prominent operational risks for firms over the past decade has been cyber-risk. The Bank of England's Systemic Risk Survey has consistently cited cyber-risk as one of the top threats to the financial system, as you can see in Figure 3.

What comes to mind if I asked you to think of a bank robber? Perhaps someone with a full-face mask and a sack?

The reality is that online fraud and cyber-hacking of digital accounts have outstripped traditional theft of banknotes and gold. Globally, cyber crime could have cost up to \$600bn in 2017 according to some estimates.⁵ Cyber-attacks in the financial sector range from those that aim to disrupt services in the short-term to those that aim to 'poison the well' by corrupting data over time.

In recent years we have seen impacts on the real economy when cyber-attacks are successful. Recent data breaches have affected customers of Ticketmaster, Equifax, and many more. At the end of last year, a ransomware attack on Travelex meant some high street banks could not take orders for foreign currency and had to handle transactions manually for an extended period.

A severe or persistent cyber-related outage or data breach which has been undetected for a long period of time can impact public trust and confidence in the financial system.

When considering operational resilience from a cyber perspective, the FPC follows similar principles to those I have already outlined for individual firms: we look at both prevention and cure.

The FPC has made Recommendations on building cyber resilience. First on prevention, that core firms and financial market infrastructures must establish a penetration testing programme (known as 'CBEST'); and secondly on cure, that these firms must also adopt cyber resilience action plans.

The FPC's primary concern is that incidents involving individual firms could escalate if they led to a broader shock to confidence among customers, or through interconnections in the financial system. In order to address this we have set out a framework for building operational resilience that includes and goes beyond the Recommendations I mentioned previously.

- i) First, the FPC requires clear baseline expectations for firms' resilience. These should reflect the importance of firms and the services they provide for the financial system;

⁵ Center for Strategic and International Studies
<https://www.financialdirector.co.uk/2018/07/16/financial-risk-analysis-methods-and-techniques/>

- ii) Second, as I've mentioned, there should be regular testing by firms, to ensure that resilience keeps pace with the evolving nature of the risk;
- iii) Third, regulators should identify firms that are not yet subject to relevant regulation, but which might be important for financial stability; and
- iv) Finally, firms should have clear and tested arrangements to respond to cyber incidents when they occur.

The next step is for the FPC is to set expectations, so-called 'impact tolerances' for how effectively critical financial companies should be able to restore vital financial services following a severe but plausible cyber incident. Consistent with the FPC's remit, these will be calibrated to ensure financial stability and avoid material economic harm. As such, these tolerances will not imply zero disruption. Regular cyber stress testing will be used to test firms' ability to meet these 'impact tolerances'.

The FPC has already done work on impact tolerances in the area of payments, another area of operational risk which I turn to now.

Payments

Payments are one of the most vital services provided by the financial system to the economy. In 2019 over 40 billion individual payments were made in the UK, with a total value of more than £90 trillion.

Payments have undergone rapid innovation in recent years, and the covid shock has accelerated these trends. In addition to traditional payments methods such as cash, cheques, and card (including online), methods such as mobile wallets like Apple Pay and contactless payments have been on the rise. In 2017 an important milestone was reached – debit card payments became the most frequently used payment method, overtaking cash, shown in Figure 4 on the slide. During the recent lockdown, data from the UK's largest cash machine network suggests that cash transactions have plummeted as online payments have increased dramatically. At their lowest, cash withdrawals were 60% lower in April 2020 than a year before.⁶

Time will tell how enduring the changes during lockdown have been. However, even before covid, the UK was amongst the most cash-light economies globally. Some economies, such as Sweden, have seen even faster rates of cash decline, as illustrated in Figure 5.⁷

⁶ LINK: Coronavirus Crisis means cash use down but UK still withdrawing £1billion from ATMs each week:

<https://www.link.co.uk/about/news/coronavirus-cash-usage-data/>

⁷ Future of Finance Report

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

As the Governor noted just last week in a speech⁸, such innovation can bring great benefits: payments are becoming faster, easier and more cost effective for people and businesses alike.

However, with great innovation comes great responsibility. We depend on payments technology more than ever. If payments technology fails, even for just several hours, there are consequences for the real economy: wages, pensions and benefits, may not arrive on time, customers can't pay for goods and services, business and household payments fail. As the Executive Director of the Bank's Financial Market Infrastructure area, Christina Segal-Knowles noted in a speech, "the ability of individuals and businesses to transact safely and smoothly is critical to financial stability. People and businesses need to be able to make and receive payments on time, with confidence, even in periods of economic uncertainty."⁹

This was one reason that HM Treasury launched a 2019 review of the payments landscape to support choice, competition and resilience and to ensure that regulation and infrastructure keep pace with innovation.¹⁰

The FPC has welcomed this review, and have committed to ensure that systemically important payment firms support financial stability, while allowing competition and innovation in payments to thrive.

In order to achieve this, the FPC has examined what risks might arise from payments innovation. In the past the payments value chain – from payment initiation, through processing, authorisation and clearing – was largely concentrated in a few entities. Payments used to be the preserve of commercial banks and core payment systems, with ultimate settlement taking place on the central bank ledger.

Now new entrants have emerged that could alter the established value chain, shown in Figure 6. These range from small businesses, to fintech start-ups (some rapidly achieving high market valuations), to big technology companies offering payment services in addition to their core business model, such as Apple.

The FPC has identified two risks in particular from these developments. First, these structural changes could lead to systemically important activities increasingly being conducted by non-banks. Second, the changes also mean that the complexity of the payments chain is increasing. Therefore it is becoming increasingly difficult for any single regulator to assess risks across the payments ecosystem.

As a result, the FPC announced last year that the current regulatory framework will need adjustment in order to accommodate innovation in payments.

⁸ Reinventing the Wheel (with more automation) September 2020
<https://www.bankofengland.co.uk/speech/2020/andrew-bailey-speech-on-the-future-of-cryptocurrencies-and-stablecoins>

⁹ 'Responding to leaps in payments' Segal-Knowles (January 2020)
<https://www.bankofengland.co.uk/speech/2020/christina-segal-knowles-speech-at-a-westminster-business-forum>

¹⁰ <https://www.gov.uk/government/consultations/payments-landscape-review-call-for-evidence>

The FPC has therefore developed the following three principles for payments regulation and supervision, which it has set out publically and communicated to HM Treasury to be incorporated in the payments landscape review.

First, regulation should **reflect the financial stability risk, rather than the legal form, of payments activities** – or said another way, ‘the same level of risk should attract the same level of regulation’.

Given the increasingly diverse nature of companies becoming involved in payments, it is important to focus on the functions they undertake, and the risks these functions pose, rather than the nature of the company itself.

Second, **payments regulation should ensure end-to-end operational and financial resilience across payment chains that are critical for the smooth functioning of the economy.**

This principle simply says that if a firm is a critical link in a payment chain, and that payment chain provides vital services to the real economy, then that firm should be regulated with a financial stability objective, as with the systemic payments systems the Bank currently regulates, shown in Figure 6.

The third principle **ensures that sufficient information is available to monitor payments activities so that emerging risks to financial stability can be identified and addressed appropriately.**

Clear, transparent regulatory expectations such as these will ensure that innovation can progress safely, avoiding serious interruptions in payment and settlement services.

Conclusion

To conclude, the FPC’s operational resilience workplan puts the real economy front and centre. Our aim is to ensure that the financial sector has the resilience to absorb, and not increase, any disruption; particularly in cyber and payment services.

The FPC - and through us the firms that provide these vital financial services - will never take operational resilience and financial stability for granted. This means that UK households and businesses can have continued confidence in the “plumbing” that provides their vital financial services, in bad times as well as good.

Thank you