Pay.UK – Written evidence (FDF0014)

As you are aware, in 2021 we processed over 10 billion transactions, worth £7.9 trillion, paying salaries, benefits, bills, mortgages and other internet and mobile banking payments, underpinning the UK economy. Our role is to ensure that payments flow safely and securely and, while APP fraud affects only 0.0066% of the volume of payments travelling through the Faster Payments System (FPS), we are acutely aware of the tragic impact it can have. We want better outcomes for ordinary people and businesses who rely on our systems.

Detection and prevention

Our first priority detection and prevention: We are working with our customers – banks, building societies and other payment providers – to help them to detect and prevent fraud before the money is sent to the criminal in a payment across our rails. Pay.UK is in a unique position to do this and we are working closely with our customers, UK Finance and the wider payments industry to tackle fraud. We also work with end user representatives, consumer groups and regulators and policymakers. By using transaction data from across our whole system, we can enable analytics functions that can support banks and building societies make real-time decisions to identify potential fraudulent activity.

We have established a fraud programme to work with the industry to tackle APP scams and other types of fraud. We are working on three fronts, both for today's Pay.UK payment systems and the New Payments Architecture (NPA):

- Development and deployment of overlays to provide our customers with tools to prevent fraud: Confirmation of Payee (CoP) is in place; others are in progress
- Working with our customers to see where our standards can add value in sharing enhanced data – we recently published the data model to support the sharing of additional data. This is a key element of the broader enhanced fraud data project we are running with UK Finance
- Potential use of our rules to support better outcomes for victims of fraud.

But there is no simple solution. Fraudsters continue to evolve their business models and we must ensure that the tools we build are flexible and adaptive to the ever-changing fraud landscape, as well as to the evolving payments architecture. All our work on fraud solutions will integrate and evolve into the final NPA delivery, which will also allow continuous development and innovation to tackle fraud.

Overlays

Overlays are a means to enable competition and innovation to optimise and improve end user experiences, working alongside the existing payment systems now, and as a core requirement of the NPA in the future. An example of an existing overlay is Confirmation of Payee.

Our fraud overlay will deliver a fraud prevention solution to market, enabling our customers access to disbursement and risk analysis tools. We are running a proof-of-concept to help us determine the right model for operating this overlay, which we expect to complete by the end of Q3 2022.

Confirmation of Payee

CoP is a name-checking service that our customers can provide to end users. It is separate to the clearing and settlement of payments, and works alongside FPS and CHAPS to give end users confidence in who they are paying. It is designed to prevent misdirected payments and can also help prevent scams where fraudsters substitute their own/different account details for those of a legitimate payee.

The Payment Systems Regulator (PSR) reports that, since its launch in 2020, CoP has improved security and strengthened end user confidence. Currently, CoP has >96% of FPS market coverage, with more than a million CoP requests every day.

Phase 2 of CoP is now live and all account holding payment providers can join the service, creating a ubiquitous capability.

Enhanced fraud data project

Our Enhanced Fraud Data project is a joint initiative with UK Finance, corresponding to the PSR's proposal to improve scam prevention through improved intelligence sharing across the industry. Pay.UK has recently published a new standard to support the exchange of data and we are now costing up a solution to deliver a service. The PSR is tracking this work through a monthly coordination group.

Checks in the payment journey

In order to have truly successful detection and prevention, we need to have better sharing of data, information and tools.

As I mentioned in my oral evidence, a fraud has already taken place by the time it hits Pay.UK's rails, so it is important for banks and building societies to have certainty of the circumstances in which they can hold a potential payment that they suspect to be a scam before releasing it to us – even if their customer wants it to be paid; or to hold funds they have received if they think that an account has been compromised by a fraudster (within reason).

If the prevention and detection tools that we are enabling are to be effective, it is necessary for institutions to be confident in their legal ability to share data and to take actions based on the insights from that data. We are aware that paying banks differ in their interpretation of the current legislation on payments processing: some exercise a right to delay or stop suspicious payments, whereas others interpret the Payment Services Regulations 2017 to mean that this is not permitted. A similar situation exists in relation to the freezing of funds by receiving banks. We support the position of UK Finance that it would be in everyone's interest for uncertainty over this issue to be removed, and for the legislation (or regulatory guidance) to make clear that such action is permitted and under which circumstances.

Reimbursement

The first priority of the industry is to detect and prevent fraud before it reaches our rails. But when fraud does happen, we support there being appropriate reimbursement for APP scams victims, consistently applied and regardless of the type of payment system.

No matter how good people, businesses and their banks get at spotting potential fraud, and at preventing scam payments being made, some will slip through. And that can be devastating for those people and businesses it touches.

We want people to know what is expected of them, and to have more clarity about whether and how they can get their money back if they have been scammed. Reimbursement is currently subject only to a voluntary code which is open to some interpretation. This can mean that outcomes for victims are on occasion inconsistent and vary from bank to bank.

As part of our discussions with Her Majesty's Treasury (HMT) and the PSR, we are exploring how Pay.UK could play a role to support the management of reimbursement, and we are also working with UK Finance to see how the timeliness of return of funds can be improved, as it currently takes up to four weeks to recover money (mis-posted or fraud). Whatever Pay.UK does as payment system operator in this area, we and the authorities will need to ensure that these activities do not pose a risk to our core payment system operations and UK financial stability.

Legislation

Lord Sandhurst asked me to write to the Committee about the work we are doing with HMT and the PSR around changing the legislation to allow consistent reimbursement for victims for fraud.

There should be a clear framework for the reimbursement by banks of their customers when an APP scam has occurred. Regulation 90 of the Payment Services Regulations 2017 indicates that if a payment was properly authorised by the payer, then the paying bank has no liability. HMT has said that it will remove the current blocks in legislation to allow for a new legal framework around liability. We have yet to see the detail of the legislation that HMT has in mind, but it should open the door for the appropriate regulator(s) to act.

We support an appropriate, clear and comprehensive liability framework with core principles set out in regulation, and with detail established by the public authorities so that all parties understand their responsibilities and rights, especially consumers making electronic payments. Given that such a framework involves the relationship between payment providers and their customers (which is generally outside of the scope of payment systems), we have previously advised HMT and the PSR that, in our view, changes to Part 5 of the Financial Services (Banking Reform) Act 2013 would also be required, if the PSR were to rely on these powers. We welcome HMT's offer to meet with us and the PSR on the detail of the proposed legislative and regulatory changes.

We would look to support banks and building societies in meeting their legal and regulatory obligations, using our rules, data standards and technology. We are working closely with HMT and the PSR to establish whether there are new responsibilities we might need to take on to do this, and to understand how any new responsibilities could be implemented with proper safeguards so not to introduce disproportionate risk to our core payment system functions, which are vital for the UK economy.

In conclusion, as I mentioned in the hearing, detection and prevention are key to tackling fraud, and we need clarity around the reimbursement of victims. We also need to work together to tackle fraud – within the payments industry and beyond, from our customers, to telecoms and social media companies, legislators and regulators. We all need to play our part in the fight against fraud as it is ever-evolving.

20 April 2022