PSR Payment Systems Regulator

Authorised push payment (APP) scams

Consultation paper

November 2021

We welcome your views on this consultation. If you would like to provide comments, please send these to us by **5pm on 14 January 2022**.

You can email your comments to **appscams@psr.org.uk** or write to us at:

APP scams
Payment Systems Regulator
12 Endeavour Square
London E20 1JN

We will consider your comments when preparing our response to this consultation.

We will make all non-confidential responses to this consultation available for public inspection.

We will not regard a standard confidentiality statement in an email message as a request for non-disclosure. If you want to claim commercial confidentiality over specific items in your response, you must identify those specific items which you claim to be commercially confidential. We may nonetheless be required to disclose all responses which include information marked as confidential in order to meet legal obligations, in particular if we are asked to disclose a confidential response under the Freedom of Information Act 2000. We will endeavour to consult you if we receive such a request. Any decision we make not to disclose a response can be reviewed by the Information Commissioner and the Information Rights Tribunal.

You can download this consultation paper from our website:
https://www.psr.org.uk/publications/consultations/cp21-10-app-scams/

We take our data protection responsibilities seriously and will process any personal data that you provide to us in accordance with the Data Protection Act 2018, the General Data Protection Regulation and our PSR Data Privacy Policy. For more information on how and why we process your personal data, and your rights in respect of the personal data that you provide to us, please see our website privacy policy, available here: https://www.psr.org.uk/privacy-notice

Contents

1 Executive summary

1.1 APP scams are a major and growing problem in the UK. As the regulator responsible for protecting people and businesses when they use payment systems, we want action to prevent APP scams and to protect people who do fall victim to them. In February 2021, we set out in a call for views three proposed measures to achieve that outcome.[1]

1.2 We have now considered the feedback received and have developed these three measures further, on which we will take action in 2022. We also set out some additional work that we want to develop in parallel to those measures.

Overview of our proposals

1.3 This document sets out our upcoming activity. We propose to:

- Require the 12 largest PSP groups in the UK (including most of the biggest High Street brands) and 2 largest PSPs in Northern Ireland outside those PSP groups to publish comparative data on: their performance in relation to levels of APP scams; reimbursement levels for their customer that are APP scam victims; and which PSPs their fraud payments have been sent to. For the first time, customers will be able to understand how well their PSP is preventing APP scams and treating the victims of fraud, and also understand which PSPs are receiving these fraudulent payments.

- Support and require industry to improve intelligence sharing, to improve detection and prevention of APP scams.

- Make reimbursement for scam victims mandatory.[2] While there could be challenges with imposing this at present, we welcome the announcement from John Glen MP, Economic Secretary to the Treasury, who has announced that the Government will legislate to address any barriers to regulatory action at the earliest opportunity. This paper sets out in more detail the two options we are considering once legislative changes have been made.

1.4 Beyond these steps, we will consider further measures by looking at what we could currently achieve, including how we could best use our existing powers. For example, this could include looking at the balance of liability between sending and receiving PSPs, to incentivise better fraud prevention and reimbursement outcomes.

1 https://www.psr.org.uk/publications/consultations/cp21-3-authorised-push-payment-scams-call-for-views/

2 Of course, consumers need to exercise caution, but we recognise that increased consumer awareness through better education by PSPs may be needed in light of the increased sophistication of scams including a rise in social engineering.

1.5 At the same time, there is value in voluntary action by PSPs to improve outcomes for customers, such as better detection and prevention of APP scams. If appropriate, we stand ready to facilitate the coordination of industry in coming together to address this significant problem urgently.

Protection against APP scams

1.6 Every year thousands of people are tricked into sending money to fraudsters in Authorised Push Payment (APP) scams. These scams can cause significant harm to victims, with many losing life-changing amounts of money. The number and cost of these scams is significant and increasing. In 2020, reported APP scam losses totalled £479m, with the actual figure likely to be higher. COVID-19 has created new opportunities for scammers and new vulnerabilities amongst consumers.

Table 1: Growth in APP scams 2019-21[3]

APP Scams	H1 2019	H1 2020	H1 2021
Cases	57,549	66,247	106,164
Losses	£207.5m	£207.8m	£355.3m

1.7 We want to prevent APP scams happening in the first place and, where they do still happen, to ensure that victims who have exercised sufficient caution have their money returned. This is essential to ensure that customers are sufficiently protected when using the UK's payment systems.

1.8 Since our work on APP scams began in 2015, there have been considerable improvements. We set up the working group that led to the industry-led Contingent Reimbursement Model (CRM) Code. The Code has been a key tool in preventing APP scams, and has led to better reimbursement rates for victims since it was introduced in May 2019. We have also directed the UK's six largest banking groups to implement Confirmation of Payee (CoP) in 2020, and have been working with Pay.UK and the industry on rolling out the service to more financial institutions. Indeed, there is evidence that Confirmation of Payee (CoP), the name-checking service designed to help people identify when payee details are not correct, has helped prevent some types of APP scams.

1.9 Although these are significant steps forward, more must be done. Levels of reimbursement vary materially across PSPs and, as participation in the code is voluntary, many customers fall outside the protections offered by the CRM code. The scale of current APP fraud – and the fact that scams are continuing to increase by total volume and total value – indicates that further work is needed to make it harder to commit these crimes.

3 UK Finance 2021 Half Year Fraud Update.

1.10 This requires coordinated action by a range of different parties. We need better protection for customers, ideally by stopping them from falling victim in the first place. We need more action on where the money is being sent. All platforms where criminals recruit their victims also need to play their part, notably large social media firms.

1.11 Within our remit and powers, the PSR continues to prioritise work on APP scams. In February 2021, we invited feedback on a proposed package of complementary measures to help reduce losses from APP scams.

Measures we're consulting on

1.12 Having developed our earlier thinking based on stakeholder feedback to our call for views, we are now consulting on our proposed next steps:

1. **Measure 1 – Publishing scam data:** The PSR will require the 12 largest PSP groups in the UK and the two largest banks in Northern Ireland outside those PSP groups to publish a balanced scorecard of data on a six-monthly basis, setting out their performance in relation to APP scams. This will include sending PSPs' APP scam rates, their rates of reimbursing customers scammed, which of those are members of the CRM Code, as well as comparative data on the wider set of PSPs receiving APP scam payments from the directed PSPs. This will provide greater transparency and incentives to improve APP scam performance. We will also publish this information in the form of a comparison of performance across PSPs.

2. **Measure 2 – Intelligence sharing:** Task industry with improving intelligence sharing between PSPs about the riskiness of payments in order to improve scam prevention. We expect to see progress on this and stand ready to act if needed.

3. **Measure 3 – Wider reimbursement:** We want all customers to benefit from reimbursement protections. As this will require legislative change, we're seeking views on the approach we could take to ensure we're ready to implement (for when we have the power to act).[4]

1.13 The causes of scams are complex and numerous. Fraudsters are sophisticated, and their methods evolve, so there is no simple solution. This is a package of measures to improve prevention and outcomes for victims.

1.14 Everyone playing a role in preventing scams needs to do more – whether this is sending and receiving PSPs or those in other sectors where these scams often originate (including social media platforms, telecoms companies and internet-related services). While our proposals are focused on our remit, we will continue engaging in the broader debate with government, other regulators and other sectors on what can be done more widely to prevent APP scams.

4 https://www.psr.org.uk/news-updates/latest-news/news/psr-announces-plans-to-stop-app-scams/

Further measures we're considering

1.15 We welcome the recent announcement from the Economic Secretary to the Treasury that the Government will legislate to address any barriers to regulatory action at the earliest opportunity. As well as preparing for potential future changes in the legislation to allow us to require reimbursement from victims' PSPs, we are continuing to look at what else we could currently achieve before legislative changes.

1.16 In addition to the three measures we are consulting on in this document, one area that we will be exploring is the appropriate balance of liability between sending PSPs and receiving PSPs. We will be developing proposals on how we could best use our existing powers – for example, looking at FPS scheme rules to understand how they compare to payment systems such as card schemes, looking at the balance of liability between sending and receiving PSPs to incentivise better fraud prevention and reimbursement outcomes, mandating further fraud prevention, or further enhancements to the CRM Code. On the latter of these, we will be exploring what enhancements could be carried out by the LSB.

1.17 There is also value in voluntary action by PSPs to improve outcomes for customers. There are additional areas we would like to explore, including voluntary action by Pay.UK and PSPs. These could include further investment in the prevention of APP scams or implementing rules (e.g. in Faster Payments) within the parameters of existing legislation. We know that a number of PSPs want to take these types of actions as a matter of priority but that coordination across the whole industry can be a challenge. Therefore, in addition to exploring these options further in our own work, we will facilitate the coordination of industry in coming together to address this significant problem urgently. We will also work with other regulators to co-ordinate actions tackling APP fraud.

1.18 While we would welcome initial views on this further work, the main purpose of this document is to consult on the three measures listed above that we plan to implement, where possible, from January 2022.

Next steps

1.19 We would like views on the three proposed measures by 14 January 2022. We welcome responses from all stakeholders and interested parties, not just those that we regulate.

1.20 Please provide your feedback by emailing us at **appscams@psr.org.uk**. We would be grateful if you could provide your response in a Word document (rather than, or as well as, a PDF).

1.21 We'll make all non-confidential responses available for public inspection. If your submission includes confidential information, please also provide a non-confidential version suitable for publication.

1.22 Following this consultation, we'll take all responses fully into account, and will set out our policy position and accompanying action on the matters discussed in this paper by H1 2022.

2 Introduction

The CRM Code has led to improvements in outcomes for APP scam victims. However, its coverage isn't universal, reimbursement levels under the Code are still relatively low and vary significantly across PSPs, and APP scam rates continue to rise. We would like to see:

- better prevention of APP scams
- higher, more consistent and more broadly applied protections for APP scam victims

Why this matters

2.1 A push payment is made when someone authorises their PSP to send money to a payee's account. In an authorised push payment (APP) scam, someone is tricked into making a push payment to a fraudster. APP scams can cause significant harm. In 2020, there were around 150,000 reported APP scam cases (an increase of 22% on 2019), with a total value of £479 million (a 5% increase on 2020). These scams have increased year-on-year since records have been kept. Many cases go unreported, so the real figures are likely higher.

2.2 Payment systems should be safe to use. We want PSPs to act to prevent APP scams from occurring, and to ensure that victims are reimbursed. So far, we have advocated industry-led approaches to this, chiefly due to statutory restrictions on the actions we can take directly.[5] In 2018, we set up a steering group of industry and consumer representatives, led by an independent chair, to develop a voluntary industry code of practice. This led to the CRM Code being introduced in May 2019.

The CRM Code

2.3 The CRM Code aims to reduce the occurrence of APP scams and to increase the proportion of customers protected from their impact, both through a reduction in APP scams and through reimbursement. The Code places responsibility on PSPs, where they are well placed to act, and on customers, where it is reasonable to expect them to take steps to protect themselves from fraud.

5 The Payment Services Regulations 2017, implementing PSD2, mean a reimbursement requirement can't be imposed on PSPs.

2.4 Before the CRM Code came into force in May 2019, there was no systematic protection for victims, with weak incentives for PSPs to work to prevent APP scams. Outcomes were uncertain and reimbursement levels were significantly lower. In its recent review of the Code, the Lending Standards Board (LSB)[6] reported that the pre-Code industry average was 19% by value in the first half of 2019.[7] This increased to 47% during 2020, for signatory banks, following the introduction of the CRM Code.[8]

2.5 In light of this, the voluntary agreement by the signatories to the CRM Code was a major step forward, setting out standards for PSPs to improve fraud prevention and victim care.

Issues with the current framework

2.6 APP scams continue to grow year on year. According to UK Finance, losses from these scams for Code signatories increased 71% during the first half of 2021, compared with the first half of 2020.[9] More needs to be done to deliver consistent and better outcomes for the victims of APP scams – and in particular to prevent scams from happening in the first place. Everyone who plays a role in the problem – including PSPs, social media and telecoms firms – has a responsibility to find the solutions.

2.7 There is also more that can be done under the CRM Code. In our Call for Views, we identified a number of concerns about outcomes under the current framework in relation to APP scams:

- Participation in the code is voluntary. Nine PSP groups, including most of the big high street banks, are signatories to the Code. Some PSPs are not offering equivalent protection or are choosing not to join the CRM Code. In relation to this, some PSPs cite difficulties in signing up to the full set of Code requirements (although this does not prevent them from offering the core protections to customers). This means that the level of protection offered to customers varies depending on where they bank.

- This difference in protections could also create potential opportunities for scammers to migrate scams from signatory to non-signatory banks if non-signatories have less relevant warnings and support in place. This is further exacerbated by the fact that many non-signatories are also not yet offering CoP.

- The overall level of reimbursement under the CRM Code has been less than 50%.[10] It is unlikely that victims have not acted appropriately in 50% of cases.[11]

---

6 The Lending Standards Board (LSB) took over the administration and governance of the CRM Code from the PSR-established Authorised Push Payments Scams Steering Group in 1 July 2019.

7 https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/01/LSB-review-of-the-CRM-Code-FINAL-January-2021-.pdf page 20.

8 UK Finance figures: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf p55.

9 https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf

10 Based on our analysis on outcomes under CRM since it was introduced on 28 May 2019 to 31 December 2020.

11 For example, compared to the rate at which appeals by victims to the Financial Ombudsman against reimbursement refusal are upheld.

- Inconsistency in Code PSPs' reimbursement rates suggests a significant variation in how they are applying the requirements of the Code. We heard during our call for views that these may result from different interpretations of the Code's exceptions regarding customers ignoring effective warnings and having a 'reasonable basis to believe' that the transaction was legitimate. The LSB and the Financial Ombudsman Service, the Code's appeals body, also noted this in their reviews of PSP performances.

- Review recommendations and case feedback from these two bodies have not been fully or consistently implemented by the PSPs. In their review earlier this year, the LSB found varying progress had been made with respect to a number of recommendations in their 2019 review.[12] The Ombudsman has also noted[13] that some firms were failing to recognise or meet their obligations under the Code, leading to legitimate claims being incorrectly declined.

2.8 APP scams continue to grow in number. This is true of Code and non-Code PSPs alike, which suggests that the Code is not providing sufficient incentives for PSPs to tackle fraud. We are mindful that the current balance of liability may mean that incentives to address mule accounts are not sufficiently strong.[14]

2.9 We have also heard concerns about how liability is allocated in the Code. Some non-PSP stakeholders believe that liability should fall more on PSPs, as they are best placed to weather the loss and prevent scams from happening. Some PSPs believe the balance should be moved in the other direction, with customers taking more responsibility for their money. The current balance of liability between consumers and PSPs was developed after extensive discussions between industry and consumer groups. We haven't seen evidence that this balance of liability between customers and PSPs is wrong. Instead, our current focus is on improving compliance with the obligations that were agreed and are reflected in the code. In particular, we want to ensure those obligations are interpreted and applied in the spirit in which the Code was drafted – on the basis that consumers who have acted appropriately will be reimbursed.

12 See the LSB's follow-up review of June 2021 on reimbursement under the CRM Code: https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/06/CRM-Review-R21c-Follow-Up-Summary-Report.pdf

13 https://www.financial-ombudsman.org.uk/files/289009/2020-10-02-LSB-CRM-Code-Review-Financial-Ombudsman-Service-Response.pdf

14 APP scams need somewhere for the scammed money to be deposited. A mule account is used by scammers to do this. They can be opened by the scammer themselves, or owned by a third party who allows the money to go through their account – sometimes not even knowing they are party to a scam.

2.10 Over time, we might expect the issues of liability to continue to be considered in light of experience. This might include greater differentiation between different types of APP scam and considering whether the balance between sending and receiving PSP is appropriate. Of course, consumers need to exercise caution[15], and we recognise that increased consumer awareness through better education by PSPs may be needed in light of the increased sophistication of scams, including a rise in the use of social engineering to get around fraud prevention measures and warnings. Action is needed by many different stakeholders, not just sending PSPs.

Key outcomes we want to see

2.11 There are some key outcomes we want to see:

- Better prevention of APP scams. The best result for customers and PSPs is scam prevention. This avoids distress, disruption and financial loss for all involved. It also prevents money ending up in the hands of criminals.

- Broader, higher and more consistent protections for victims of APP scams. All customers should enjoy the same protections, regardless of their PSP.

2.12 There are also other ways that the industry can act to improve outcomes for customers – for example, through further investment in APP scam prevention, or by implementing new scheme rules. We are aware of the existing desire in the industry to act on these matters, although coordination can make this difficult. We will therefore endeavour to act where we can to help with this coordination. In Chapter 6, we are setting the further areas of work we will be considering in 2022.

This consultation

2.13 The rest of this consultation paper is set out as follows:

Chapter 3 details the responses to the call for views we published in February, and our assessment of the points made in these.

Chapter 4 sets out the comparative data on APP scam performance that we are proposing to require PSPs to publish under Measure 1.

Chapter 5 describes our proposal to task an existing industry working group with delivering concrete proposals and associated rules and standards on sharing risk information.

15 This is one of the regulatory principles that the PSR must have regard to in discharging its general functions, under section 53 of the Financial Services (Banking Reform) Act (FSBRA).

Chapter 6 develops further the two options from our call for views paper, to address the currently limited coverage of protection for customers from APP scams under the CRM Code. It also sets out further areas of work we will be exploring in 2022.

Chapter 7 sets out the timetable for this consultation and the steps we intend to take following this.

Chapter 8 contains our cost-benefit analysis of the requirements we propose to impose on PSPs under Measure 1.

Chapter 9 sets out our assessment of the likely equality impacts and rationale for the measures we are proposing, in line with our public-sector equality duty under the Equality Act.

Chapter 10 contains a draft of the direction we are proposing to use to implement Measure 1.

3 Our call for views

In February 2021, we published a call for views inviting feedback on outcomes under the current framework as well as on three potential complementary measures to address the problems outlined in the previous chapter. We received 51 responses, from a wide variety of stakeholders.

Having considered these responses, we have concluded that:

- Industry participation in the fight against APP scams – whether through membership of a code or a requirement in scheme rules – should be broadened to all PSPs.
- We have seen no evidence from the responses that the balance of liability between consumers and PSPs in the CRM Code is wrong. Over time, we might expect the issues of liability to be considered in light of experience.
- The Code's rules need to be applied consistently and correctly by all Code members.
- Comparisons between PSPs' APP scams performance against a balanced scorecard should be published.
- We propose harnessing existing industry activity to develop transaction risk information sharing.
- We should continue to consider how and whether to implement mandatory reimbursement for APP scams. While there could be challenges with imposing this at present, we are working with HMT to input into legislation that would allow us to use our powers to impose reimbursement if appropriate.
- At the same time, we are continuing to look at what we could currently achieve on reimbursement, including how we could best use our existing powers.

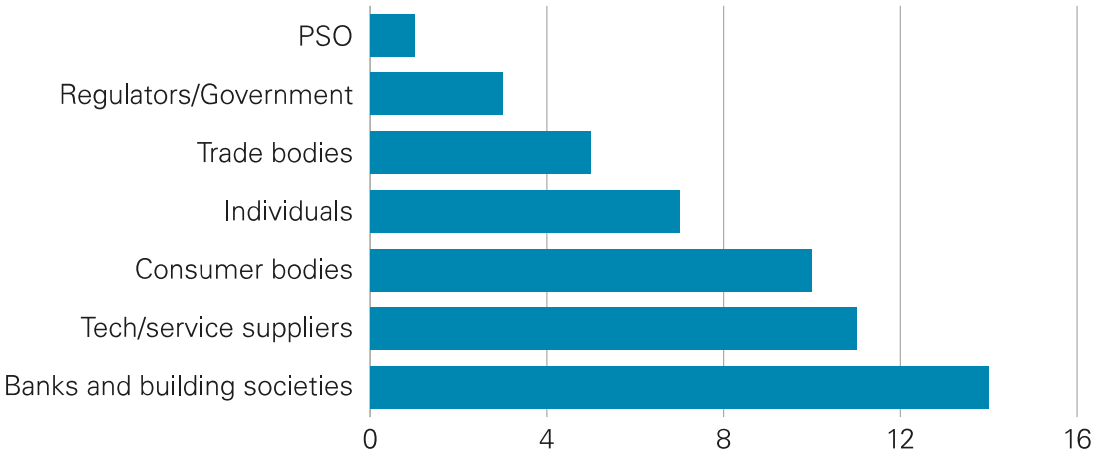
3.1 Our call for views in February 2021 invited feedback on current APP scam data and on three complementary potential measures to prevent APP scams and protect victims:

- Improving transparency on outcomes, by requiring PSPs to publish comparable data on their APP scam, reimbursement and repatriation levels.
- Improving the detection and prevention of scams by requiring PSPs to adopt a standardised approach to risk-rating transactions and to share the risk scores with other PSPs involved in the transaction.
- Broadening and strengthening APP scam protection, by requiring all payment firms using Faster Payments to reimburse victims of APP scams.

Responses to our call for views

3.2 We received 51 responses to our call for views. Most were from PSPs and financial technology and service providers. We also received responses from consumer bodies, industry trade bodies, private individuals, regulatory/governmental bodies and a payment system operator. We will publish the non-confidential responses separately.

Figure 2: Responses to our February 2021 Call for Views



Respondents' views on the current situation

3.3 The first five questions of the call for views concerned the current levels of APP scams, and the functioning of the CRM Code. We asked what might be driving these outcomes, what might be the appropriate balance of liability among banks and customers, and how to ensure consistency and transparency in outcomes.

APP scams are growing, and the Code needs to be improved and broadened

3.4 There was an overall consensus that the CRM Code membership should include more PSPs. PSPs pointed out that scammers are changing their behaviour by using non-Code PSPs to receive scammed money, including because of the general lack of safeguards such as Confirmation of Payee.[16]

3.5 Some PSPs pointed out that outcomes for victims had improved since the CRM Code had been in place, and that the data we published did not show scams avoided or prevented. PSPs added that any available figures for this latter measure would be likely to be significantly under reported.

16 The CRM Code is voluntary, whereas CoP was mandated by a specific direction on the UK's six biggest banking groups. There is a significant overlap between the PSPs adopting the two measures, but the Code itself doesn't include CoP as a requirement.

3.6 Some respondents said that the Code is unsuited to non-bank PSP business models, and that it would need to be modified to include many non-bank PSPs.

3.7 One regulatory/governmental respondent noted the need to balance widening the range of PSPs able to become signatories to the Code against ensuring there is a consistency and minimum standard in the protections provided by it.

Our response: the need to broaden participation in the industry's joint activity against APP scams is very important.

3.8 While the current CRM Code covers the large majority of customers and their payments, there are benefits to these standards being applied more broadly – ensuring that all customers benefit from these protections and mitigating the potential risk of fraudsters migrating from Code signatory to non-Code signatory banks. It is therefore essential that any measures we put forward should ensure this. The Code needs to be applicable to a wider range of PSPs if this is to be achieved. However, we note that it is also open to PSPs to offer equivalent protection to the CRM Code to their customers. Indeed, one PSP (TSB) has taken this approach. The current inflexibilities of the CRM code are not, therefore, an obvious barrier to all PSPs offering equivalent protections for their customers.

There was disagreement on the current balance of liability in the Code

3.9 PSPs generally thought that the focus of liability had 'moved' towards PSPs over the period since the Code's implementation, and that there needed to be more focus on customer liability in APP scams – as consumers do have a general responsibility for their decisions. Consumer bodies tended to think that liability should sit more with those stakeholders better able to bear the (often significant for an individual consumer) cost of APP scams – that is, the PSPs.

3.10 Both types of respondent focused on the interpretation being given to the rules of the Code, rather than the balance of liability set out in those rules. For example, nobody argued against the requirement that the customer should have a reasonable basis to believe the transaction was genuine; the arguments were about how that rule should be interpreted.

3.11 A number of different types of respondent thought that there should be a better balance of liability among the PSPs involved in scam transactions – that is, sending and receiving PSPs – as both of these have responsibility for the scam taking place.

3.12 Some PSPs stated that there was a growing number of relatively low-value purchase scams, and that these should be ruled out of scope for the CRM Code, as they were not the type of thing that the Code was drafted to address.

Our response: we haven't seen any evidence to suggest that the balance of liability between consumers and PSPs in the Code should be changed.

3.13 Although PSPs and consumer bodies each argued for re-balancing liability in different ways, we have not seen any evidence for altering the balance of liability between consumers and PSPs in the Code in a particular way. Notably, parties on both sides of the discussion did not question the drafting of the Code but raised concerns over its application.

3.14 We think it would be more effective to work towards better application of the Code, rather than re-open the long debate about liability from when the Code was drafted. It may be the case that there needs to be more clarity about how PSPs should interpret those rules.

3.15 Lastly, further discussions may need to take place to consider the scope of any future code, as part of the overall continuing development of measures put in place to combat APP scams, whether by industry or as part of future regulatory action. This could include looking into the balance of liability between the sending and receiving PSPs in APP scams, and whether this should be changed. We explain this further in 6.25.

The Code is too open to interpretation and there needs to be further clarification on its implementation

3.16 There was a consensus across a range of stakeholder types that the provisions of the Code needed to be clarified. However, there were two opposing views on why and how this should be done: PSPs felt that the interpretation of the CRM Code has had the effect of focusing liability onto banks, and that there should be clearer responsibilities for all parties (including customers). Conversely, consumer bodies felt it was insufficiently clear that banks should reimburse victims, and that there should be a clearer general responsibility on them to do this.

Our response: although there is sufficient clarity in the CRM Code rules, they need to be applied as intended.

3.17 In the responses to our call for views, there were comments from different stakeholders that the balance of liability between customers and PSPs resulting from cases considered under the Code were not reflecting the intended balance when the Code was drafted. Despite this, we have not seen any evidence in the responses demonstrating a need to change the balance of liability between PSPs and customers in the CRM Code. We therefore think that the problem lies in how the rules are being applied.

3.18 We nevertheless understand the requests for clarification. It may be the case that further guidance on the application of the CRM Code's provisions is needed. While this could lead to more consistent outcomes, we believe that any such guidance would have to be provided by the LSB and the Financial Ombudsman, rather than the PSR.

3.19 A governmental respondent representing several government entities warned that the Code sets out a non-exhaustive list of circumstances to be taken into account when assessing APP scam claims, and that any cases should be looked at in terms of all their circumstances. It is also clear from many of the decisions of the Financial Ombudsman that there is a need for PSPs to consider all relevant factors in APP scam claims, particularly given the growth in the social engineering of victims – we want this to continue.

Respondents' views on our proposed measures

3.20 In the call for views, we set out three measures we thought could help prevent APP scams and protect customers who do fall victim. We asked stakeholders what they thought about the measures, including their effectiveness and proportionality.

There were a number of different opinions on what data should be published and who should do it.

3.21 We proposed Measure 1 to improve transparency. It requires PSPs to publish data on scam, reimbursement and repatriation levels. This would give consumers information to help them choose their PSP, and to give PSPs a reputational incentive to improve their performance.

What data should be provided

3.22 PSPs were generally against 'naming and shaming' by the publication of APP scam reimbursement rates alone, which might not fully represent a PSP's efforts. Most respondents thought the data published should be a 'balanced scorecard' including some measure of a PSP's efforts to prevent scams, as well as how much they reimburse scammed customers. There was a consensus across respondents that the data published should also refer to receiving banks, as they play a significant role in APP scams taking place. Some respondents wanted to see PSPs' rates of appeal to the Ombudsman (and outcomes), the amounts borne by victims, the time taken by PSPs to deal with claims, and the number of scams (and amounts lost) originating outside of the banking industry.

Who should provide their data

3.23 There was general consensus that those required to publish should not be just the larger PSPs, or current CRM Code signatories, but that all PSPs should be included in any requirement to publish data. This was to avoid a 'naming and shaming' exercise which affects only some PSPs, and also to give customers fuller information with which to make their choices. Some PSPs also suggested this might highlight the trend for APP scams involving non-Code and non-CoP banks.

Who should collate and publish the data

3.24 There was no consensus on who should do this. The suggestions ranged considerably, from UK Finance, to the LSB, the Financial Ombudsman, Pay.UK, the PSR and the Home Office.

Possible unintended consequences

3.25 Some PSPs (but also some other respondents) argued that publishing reimbursement data could encourage customers to take less care or even more first-party fraud (where the 'victim' is complicit in the APP scam). There was also a general concern that the data published shouldn't help fraudsters, by highlighting possible deficiencies in some PSPs' anti-fraud systems.

Our response: a balanced scorecard of PSPs' performance relating to APP scams should be published.

3.26 It is important that a clear indication of PSPs' performance should be published. This will inform customers and also provide reputational incentives, as set out above. There are benefits of having a broader set of banks publish APP scam comparative performance data, to increase the consumer information and incentives on sending (and receiving) banks, as well as to ensure a level playing field. However, we also recognise that any intervention needs to be proportionate and take account of how quickly banks can implement this policy to ensure an effective remedy. We set out in Chapter 4 our proposal for which PSPs we consider should be required to provide their APP scams data.

3.27 We agree with the importance of including data relating to the performance of both sending and receiving PSPs. Indeed, it is the receiving PSPs that are providing accounts for the scammers, and by publishing their performance we want victims to understand which PSPs are receiving these fraudulent payments.

3.28 The set of data to be published should be what is necessary and sufficient to provide a clear and balanced view of the performance of PSPs on the key metrics of concern to consumers and other stakeholders. We think directed PSPs should publish data comparisons – produced by the PSR using data provided by those PSPs, of their performance against other PSPs – prominently on their websites. This should include both other directed sending PSPs and a wider set[17] of PSPs receiving APP scam payments from the directed PSPs. The comparisons should also be published by the PSR. Other organisations, such as industry and consumer bodies, would be able to use and republish the comparisons themselves.

3.29 Publishing data on the platforms where APP scams originate (mobile, search engine, social media, etc.), and potentially data on individual platforms, could highlight where issues are, inform consumers and provide reputational incentives on these wider stakeholders to prevent scams. We support banking industry initiatives to publish data on the types of sources of scam origination.[18] While Measure 1 is designed to provide a balanced comparison between individual PSPs' APP scam performances, to provide reputational incentives on PSPs to make improvements, there could be real value in the industry designing and publishing similar balanced comparisons of individual platforms'

17 For details of how this wider set of PSPs will be determined, see Box 3 in Chapter 4.

18 See, for example, UK Finance's published information on this: https://www.ukfinance.org.uk/press/press-releases/over-two-thirds-of-all-app-scams-start-online%E2%80%93new-uk-finance-analysis

and other originators' performances on APP scams. We will engage with the industry and other regulators on whether and how this can be facilitated.

3.30 We have considered the points made by some stakeholders about the possibility of unintended consequences from requiring publication of certain data, such as APP scam levels by bank. Given the sophistication of many scams, we consider it likely that scammers are already aware of those banks which are being disproportionately targeted. PSPs will have time to address any weaknesses ahead of the publication of data.

3.31 Furthermore, we have seen no convincing evidence or arguments that publishing PSPs' levels of reimbursement under Metric A would lead customers to take less care when making payments. Being scammed is always distressing, and publishing PSPs' reimbursement performance will not signal to customers that they will always be reimbursed.

3.32 We set out in the next chapter what data we propose PSPs should publish on APP scams.

There was widespread support for transaction risk information sharing – but not in the form we proposed

3.33 In the call for views, we noted that greater sharing of risk information between PSPs involved in a transaction could help prevent APP scams. We proposed that one way of doing this could involve generating a risk score for each transaction. The information could form part of the payment message and be passed automatically between the sending and receiving banks, possibly using existing fields in a payment message to provide a numerical risk rating score.

3.34 There was significant agreement, across multiple respondent types. Many believed, however, that significant time would be taken up in agreeing how to code a risk score from the available data points. They also felt it would be difficult to interpret what a numerical score could mean, which factors were driving the score, and that an overarching numerical score might miss important factors that would be available in the underlying information.

3.35 Many respondents suggested a better alternative might be to develop industry-agreed principles for the two-way sharing of specific elements of data, at strategic points within the payment journey. This could use APIs outside the transaction (rather than within the payment message, which may not have space) and could therefore include other data – for example, highlighting suspected mule accounts to receiving PSPs. PSPs thought this should be mandated to all PSPs.

Our response: we support the alternative approach proposed by stakeholders.

3.36 In response to our call for views, PSPs pointed out that the existing industry initiative intended to improve real-time information exchange concerning transaction risks could potentially be more forward-looking and flexible than using the existing payments message technology (as suggested in the call for views) and would offer richer data exchange. We set out in Chapter 5 how we intend to task this working group to produce a solution.

PSPs wanted to retain the CRM Code, but make it mandatory; non-PSP respondents thought an obligation to reimburse in scheme rules would be better

3.37 The third measure we proposed involved broadening and strengthening APP scam protection, by requiring all payment firms to reimburse victims of APP scams. We set out two potential approaches – measure 3A, which proposed incorporating the obligation to reimburse into scheme rules; and measure 3B, which proposed introducing a requirement to be a member of an approved code.

3.38 Regarding measure 3A, non-PSP respondents were generally in favour of a stronger obligation on all PSPs to reimburse victims. There was also a desire that this should include an improved version of the CRM Code's requirements. PSPs (and some technology and service providers) argued that this would have reduced scope for customer liability (and bring problems of recklessness), with many expressing concerns about the ability of Pay.UK to enforce such a rule.

3.39 The costs of reimbursement were highlighted by some PSPs as significant for the industry, especially if reimbursement were to be increased. This was said to be particularly the case for smaller PSPs.

3.40 There was more support from PSPs on measure 3B; however, many seemed to see this as a chance to 'reset' standards away from 'automatic' reimbursement, towards increased liability for victims. There was also broad support for broadening participation in any code, and for clarifying the liability for receiving banks.

3.41 Others (including some consumer bodies) saw option 3B as at risk of replicating the existing problems they saw with the Code.

3.42 There were concerns raised about the ability of Pay.UK to implement and enforce both options in its system rules.

Our response: there are merits in both 3A and 3B, and we want to consult further on these.

3.43 We have heard arguments for and against both measures 3A and 3B. We believe more detailed discussion would be useful at this stage. We set this out further in Chapter 6.

3.44 We consider it important to introduce mandatory reimbursement requirements for all customers who have exercised sufficient caution, so that these protections are available to all customers – irrespective of their choice of PSP.

3.45 We have seen no compelling evidence that mandatory reimbursement will cause customers to be careless with their payments. In fact, PSPs that have introduced blanket victim reimbursement policies have told us that this did not result in any increase in claims. However, we agree that consumers need to exercise caution but recognise that increased consumer awareness through better education by PSPs may be needed in light of the increased sophistication of scams.

3.46 We recognise that reimbursement costs for PSPs could be significant under both scenarios – particularly for smaller PSPs that are currently not signed up to the CRM Code – and we will take this feedback into account. However, a key aim of the policy is to incentivise PSPs, including receiving PSPs, to invest more in scam prevention. Ensuring that they bear the costs of reimbursing customers who have exercised sufficient caution is instrumental to this.

3.47 We recognise concerns that the existing legislation and Pay.UK's governance could both impact the effectiveness of any reimbursement requirement imposed through change to scheme rules. In our recent draft PSR Strategy, we have stated that we support developments to Pay.UK's governance with a view to giving it a stronger role to lead the development of protections afforded in interbank systems, coordinating its participants where necessary. This may point to the need for further evolution of Pay.UK's current role, and whether there would need to be any changes to its resourcing model and governance.[19] We note concerns about an inappropriate reduction in the levels of protection afforded to customers. However, as the PSR would need to approve any Code, this would mitigate the risk of this happening.

3.48 We therefore continue to consider that reimbursement for scam victims should be made mandatory. While there could be challenges with imposing this at present, it is useful to explore the two options further to ensure we are ready to act as soon as it becomes possible. This is an important issue, and we need to get the solution right.

3.49 As well as looking at possible ways to require reimbursement from customers' PSPs under changed legislation, we are continuing to look at what we could possibly achieve before legislative changes, including how we could best utilise our existing powers.

19 https://www.psr.org.uk/publications/general/our-proposed-strategy/

4 PSP data on APP scams

Following our call for views, we have concluded that publishing a balanced scorecard comparing data on PSPs' performance on APP scams will provide reputational incentives for PSPs to prevent APP scams and protect and reimburse victims. We are consulting on requiring reporting of data and publication of comparisons between PSPs on the following metrics:

- Metric A: The proportion of APP scammed customers who are left – fully or partially – out of pocket.
- Metric B: Sending PSPs' APP scam rates.
- Metric C: Receiving PSPs' APP scam rates, net of repatriation. Those comparisons will also include the wider set of receiving PSPs to whom the directed PSPs send payments.

We propose to direct the 12 largest PSPs in the UK and the two largest banks in Northern Ireland outside those PSP groups to report this data and to publish comparisons between PSPs (based on our collation of the data reported), including Metric C comparisons involving the wider set of PSPs receiving APP scam payments from the directed PSPs. We will consider extending the requirement to more PSPs over time.

We propose to implement a trial run of Measure 1 data reporting and presentation (without publication), on a voluntary basis prior to us issuing our direction, to help refine processes.

Our proposal

4.1 In the previous chapter, we summarised the responses we received to our call for views, as well as our response to these. We have taken the responses into account in our proposals for Measure 1.

4.2 We also commissioned a review by consultants Lucerna Partners to recommend the best metrics to use for Measure 1, and to consider issues related to the implementation of Measure 1. We are publishing their report separately. We have taken its recommendations into account, and built on them, in developing our detailed proposals set out below.

The aim of publishing APP scam data by PSP

4.3 The outcome we are seeking from Measure 1 is a reduction in APP scam losses incurred by customers, both through preventing scams and ensuring customers are appropriately reimbursed.[20] The purpose of Measure 1 is to make clear, easily accessible and comparable data about individual PSP APP scam performance available to consumers and other stakeholders. We expect this to provide strong reputational incentives on PSPs to reduce APP scam losses incurred by consumers, both through preventing APP scams and reimbursing those who are scammed.

4.4 We see the incentives on PSPs arising in the following ways:

- Consumers and other stakeholders become more aware of which PSPs are better or worse performers on consumer losses from APP scams. Consumers may find comparative data published on PSPs' or the PSR's websites, and consumer bodies and consumer journalists may use the published data to interpret, interrogate and publicise PSPs' performance.
- Greater awareness by consumers can affect their choice of PSP, because they wish to protect themselves from the risk of APP scam losses or because they are ethically concerned about those PSPs most involved in enabling funds to flow to criminals. We note, however, current limited levels of bank account switching.
- Greater public awareness of PSPs' relative performance of APP scams has an impact on PSPs' reputation with a range of key stakeholders, including government, politicians, investors, journalists, employees and regulators, as well as customers. This could lead to adverse impacts for PSPs seen to be poorly performing.
- Measure 1's impact on consumer choice and on a PSP's reputation will incentivise greater focus by the sending and receiving PSPs' boards on reducing consumer losses from APP scams.

What metrics should be published?

4.5 The data metrics published as part of Measure 1 need to achieve the intended reputational incentives. The metrics proposed are informed by the work we commissioned from Lucerna's detailed interviews with a range of stakeholders and the responses to our call for views.[21] They considered a range of potential data metrics and assessed these against criteria for their likely incentive effect, fairness of comparisons between PSPs, practicality and potential for unintended consequences.

20 Measure 1 is focused on reducing APP scam losses to consumers and micro-businesses, rather than larger corporates.

21 For example, Lucerna assisted in the preparation of the original 2016 Which? super-complaint into APP scams, and have carried out numerous other assignments in financial services and payments. https://www.psr.org.uk/how-we-regulate/complaints-and-disputes/which-super-complaint-on-payment-scams/

4.6 An effective reputational incentive would focus on the information that is most relevant to consumers. In principle, a consumer is likely to care most about the following:

- How likely is a PSP to give me my money back if I am a victim, compared to other PSPs?
- How likely is a PSP to protect me from falling victim to an APP scam, compared to other PSPs?
- How much is a PSP involved in enabling people's money flow to criminals, compared with other PSPs?

4.7 Based on the recommendations we have received from Lucerna, we propose that Measure 1 comprises these data metrics:

Metric A: The proportion of APP scammed customers who are left – fully or partially – out of pocket

- By volume: total APP scam cases where the cost is fully or in part borne by the victim, as a percentage of all the sending PSP's APP scam cases; and
- By value: total value of APP scam losses borne by victims, as a percentage of sending PSP's total APP scam value.
- Data would be split by scam value (in bands – for example, scams of £0-£1000, £1000-5000, etc) as well as in total.

Metric B: Sending PSPs' APP scam rate

- By volume: total number of APP scam payments by consumers, as a percentage of total number of push payments by consumers; and
- By value: total value of APP scams involving consumers, as a percentage of total value of push payments by consumers.

Metric C: Receiving PSPs' APP scam rate, net of repatriation

- Total value of APP scam payments received from consumers minus the value repatriated, as a percentage of total value of push payments received from consumer accounts.

4.8 We propose to direct a set of PSPs to provide the data needed to publish comparisons between those PSPs under each metric. For Metric C, those comparisons will also include certain PSPs within the wider set of receiving PSPs to whom the directed PSPs send payments. The basis on which the PSR would select the receiving PSPs discussed further in the next section.

4.9 We also propose to require directed PSPs to indicate, alongside the published comparisons between PSPs, whether or not each PSP is a signatory to the CRM Code.

4.10 This simple, limited set of data metrics provides a sufficiently balanced picture of PSPs' performance. It shows both where APP scams occur and how PSPs perform in reimbursing APP scams. It also reflects the role of both sending and receiving PSP. At the same time, it focuses clearly on the key information of concern to consumers and wider stakeholders.

4.11 Metrics A and B – the likelihood of a consumer being scammed and of being left out of pocket (fully or partially) if they are scammed – are highly relevant for consumers considering where to bank and to the wider reputation of a PSP. There could be a linkage between these two metrics – better performance on preventing scams could in principle lead to lower levels of reimbursement. Publishing data on these metrics together will help ensure a fair and balanced overall picture.

4.12 The modest additional complexity of presenting Metric A data split by scam value band is justified by providing valuable additional information to stakeholders, including on how PSPs handle reimbursement of the highest value, most potentially life-changing, scams. We are seeking views on the appropriate scam value bands, noting the need to limit complexity by restricting the number of bands – for example, to three bands, and potential benefit from the upper band capturing the range of sums that may be life-changing given the range of consumers' economic circumstances.

4.13 We have seen no convincing evidence or arguments that publishing PSPs' Metric A performance data would lead customers to take less care when making payments. Publicising current levels of reimbursement by Code PSPs would not give consumers high confidence of getting their money back. Furthermore, being a victim of a scam is distressing enough, regardless of any reimbursement. Even if very high levels of reimbursement were achieved, consumers would be unlikely to take greater risks with significant sums.

4.14 Metric C is particularly relevant to a PSP's wider reputation – showing how far a PSP is playing its part in preventing scams, protecting customers of other PSPs and limiting flows of funds to criminals, and could also contribute to some consumers' choice of PSP.

4.15 We are not persuaded that publication of Metrics B and C would give material aid to scammers. Data suggesting a PSP is being disproportionately targeted by scammers seems unlikely to be telling scammers anything they are not already aware of. If PSPs have existing weaknesses, they have well over a year to resolve them before the first Measure 1 data will be published. If new weaknesses are identified during a Measure 1 reporting period, our proposed timetable for publication (see below) gives time for them to be addressed. Given the importance of this issue, we are interested in evidenced views on our proposed timetable.

4.16 Lucerna reviewed other categories of data that could be included in Measure 1 but did not recommend any of them.

- The Financial Ombudsman's data on numbers and outcomes of complaints about APP scams is highly relevant, but the Ombudsman can publish this data and it is not necessary or appropriate to include it in Measure 1.

- We support banking industry initiatives to publish data on the wider facilitators of APP scams, such as social media platforms and telecoms systems. There could be real value in the banking industry designing and publishing comparisons of individual platforms' and other originators' performance on APP scams. We will engage with the industry and other regulators on whether and how this can be facilitated, bearing in mind the statutory remit of the PSR. Measure 1, designed to compare and incentivise PSPs, is not the appropriate mechanism for publishing this data.

4.17 We propose that the scope of payments to be covered by Measure 1 is authorised push payments to UK recipients made using Faster Payments because the vast majority of APP scam payments are made over the Faster Payments system. Our draft direction reflects this.

4.18 APP Scams may also happen in relation to payments within the same PSP group, where the sending and receiving PSPs are part of the same group. Such payments are referred to as 'on-us' payments. We propose that PSPs should also voluntarily include such scams and payments within their reporting. Victims are impacted, whether the scam is on-us or not, and inclusion in the data will facilitate consumer choice and contribute to the reputational incentive under Measure 1. We will be fleshing out the details for how to include these transactions during a trial of Measure 1 – we set out our proposals for this trial below.

4.19 Annex 3 contains the draft direction implementing Measure 1. This sets out the proposed metrics that PSPs must publish, and implements other requirements that are part of Measure 1.

Questions:

1. **Do you have comments on our proposed data metrics?**
2. **Do you have comments on the proposed scope of payments included in Measure 1?**
3. **Do you have views on the scam value bands for Metric A data?**
4. **Do you have any comments on the draft direction at Annex 3?**

Which PSPs' performance data should be published?

4.20 In responding to our call for views, many stakeholders called for the Measure 1 requirement to be imposed as widely as possible across PSPs, because there should be a level playing field between PSPs, and because APP scams have recently been migrating from Code signatories and CoP providers to a wider group of receiving PSPs.

4.21 We agree that a broad coverage of Measure 1 would deliver the most benefits. At the same time, we want Measure 1 comparisons to be published as soon as possible, and our regulatory requirements need to be proportionate.

4.22 We propose to direct the 12 largest PSP groups, in terms of payments sent, to report and publish Measure 1 data. Specifically, we propose that the directed PSPs:

- report data under Metrics A-C, including Metric C data on the receiving banks to whom they send payments; and
- publish comparisons of their performance with the performance of other PSPs, which for Metric C will include a wider set of receiving PSPs to whom payments are sent by directed PSPs.

4.23 The 12 largest PSP groups are:

- Barclays (comprising Barclays Bank UK plc and Barclays Bank plc)
- HSBC (comprising HSBC Bank plc and HSBC UK Bank plc)
- Lloyds Banking Group (comprising Bank of Scotland plc, Halifax and Lloyds Bank plc)
- Metro Bank plc
- Monzo Bank Limited
- NatWest Group (comprising National Westminster Bank plc, Royal Bank of Scotland plc and Ulster Bank Limited)
- Nationwide Building Society
- Santander UK plc
- Starling Bank
- The Co-operative Bank
- TSB Bank plc
- Virgin Money UK PLC, including Clydesdale Bank.

4.24 These groups include most of the UK's biggest High Street retail banking brands. In the first half of 2021, the 12 largest PSP groups accounted for over 95% of Faster Payments sent, both by number and by value, and the vast majority of APP scam payments sent over Faster Payments (as reported by UK Finance members). We also propose to direct AIB (Northern Ireland) and Northern Bank Limited (t/a Danske Bank), who have significant consumer businesses in Northern Ireland, in order to ensure adequate coverage in this country. Together with the 12 PSPs (which include Ulster Bank, as part of the NatWest Group), these 14 PSPs account for over 50% of consumer current accounts in Northern Ireland. This is a proportionate regulatory requirement, and by directing these PSPs we cover the vast majority of payments. We will consider expanding coverage of Measure 1 in due course.

4.25 We will consider whether the timescale for compliance with the direction should vary between directed PSPs. Those PSPs that are Code signatories and CoP providers already collect most of the data we propose for publication. We would welcome views on how long it will take other directed PSPs to put in place the necessary reporting systems.

4.26 The selection of PSPs to be included in the Measure 1 direction is based on PSP size, rather than membership of the CRM Code. This avoids any risk of disincentivising PSPs from joining the Code in order to avoid the Measure 1 requirement.

4.27 We propose to require the directed PSPs to report Metric C data to the PSR on all receiving PSPs to whom they sent payments. This is the most practical approach because:

1. sending PSPs have the information, from their investigations, about whether a payment is an APP scam
2. sending PSPs also have the information on the total value of payments sent to each receiving PSP from accounts held by consumers
3. such a reporting requirement on the 12 largest PSPs alone could, when collated, provide representative Metric C data on all receiving PSPs

Our approach to Metric C reporting therefore enables comparisons of as many receiving PSPs' APP scam performance as we choose to publish.

4.28 We recognise that some PSPs, in addition to those we direct, may wish voluntarily to be included in our published data comparisons under Metrics A and B. We propose to allow this, provided such PSPs opt-in to both Metrics A and B and comply with the relevant arrangements specified in our direction. We consider this could be done administratively and does not require specific provision in a PSR direction.

Questions:

5. Do you have comments on our proposal for which PSPs should initially be required to report and publish Measure 1 data?

6. Do you have views on how long it will take directed PSPs to put in place the necessary reporting systems?

7. Do you have comments on our proposal to allow PSPs to be voluntarily included in published data comparisons?

How and where should the data be published?

4.29 It is important that PSPs' performance on APP scams is published in a consistent way that enables easy comparison. We propose that the PSR will determine the presentation of, and publish, the comparisons between the directed PSPs (and any voluntarily participating PSPs) under Metrics A and B, and between a wider group of receiving PSPs under Metric C. More detail on how we propose to do this is in Box 3.

Box 3: Publishing APP scam data

Directed PSPs will provide to the PSR their own performance against Metrics A-C. The PSR will use this information to prepare comparisons of the performance of PSPs under Metrics A-C.

Directed PSPs will also provide to the PSR information about the performance under Metric C of all the PSPs to which they have sent APP scams. The PSR will then decide which receiving PSPs to include in that reporting cycle. We propose to do this by setting a de minimis threshold in each reporting cycle, using consistent and transparent criteria. Only PSPs above this threshold would be included. We propose the principal criterion for setting the threshold would be the total number of payments received by a PSP. In setting the threshold, we might also include PSPs' numbers of payments relating to APP scams, the value of APP scam payments and/or the value of total payments received. We would set the threshold so that, in each reporting cycle, we would include a set of PSPs that together receives the vast majority of FPS payments.

We are aware that the PSR's decision could have significant implications for affected receiving PSPs. We also intend to publish our criteria in guidance, which will be updated from time to time.

Receiving PSPs that are included in Metric C in a reporting cycle will have a chance to review the data relating to them before publication, to help ensure its accuracy. Further detail of this is set out in Box 4 below.

4.30 We propose that directed PSPs (and any voluntarily participating PSPs) publish the same or a very similar presentation of comparisons under Metrics A to C, in a form specified by the PSR. It would not be proportionate to require the wider group of receiving PSPs, only included in published comparisons under Metric C, to publish those comparisons, given the expected limited impact of Metric C comparisons alone on customer switching decisions.

4.31 We will develop a template for the presentation of comparisons between PSPs. We note the presentation of published comparisons of the service quality survey results for major banks, following the Competition and Market Authority's retail banking market investigation.[22] We will consider approaches to presenting comparisons of metrics A to C most likely to be meaningful and helpful to consumers and other stakeholders.

4.32 We propose to publish comparisons between PSPs at PSP group level. We will indicate clearly which consumer brands form part of each PSP group. We have considered publishing data comparisons between all the separate consumer brands operated by the directed PSPs, but this additional complexity would not be appropriate, given the likely degree of commonality of payment processing systems and safeguards across each PSP group. Differences between customer bases at brand-level could also make it harder to compare PSP performance.

22 Independent service quality survey results, as published on Lloyds Bank's website.

4.33 We propose to require directed PSPs to publish the data comparisons we specify in a prominent position on their consumer web pages. This means a consumer could be expected to notice the data if searching for information about opening or switching a current account or using current account services. We welcome views on this.

Questions:

8. **Do you have comments on how and where data comparisons between PSPs are published, including our proposals to compare PSPs at PSP group level?**

9. **Do you have views on the basis we use for determining which receiving PSPs are included in published Metric C comparisons?**

10. **Do you have comments on our proposal for the preparation and validation of information about receiving PSPs?**

11. **Do you have comments on how we specify where PSPs must publish the data on their websites?**

When should the information be published?

4.34 We propose to require directed PSPs to report Measure 1 data to us every six months on those APP scams notified to the PSP during the previous half calendar year period. We propose to require comparisons between PSPs' performance to be published between six and seven months in arrears. For example, data comparisons published in January 2023 would be based on data reported by PSPs for the period 1 January to 30 June 2022.

4.35 This proposal is appropriate for a number of reasons:

- It provides a sufficiently up-to-date overview of PSP performance, while giving them time to make material progress on any issues.
- The reporting period is sufficiently long to limit the impact of any short-term fluctuations in the data, such as particularly large scams, which could otherwise reduce the effectiveness of comparisons.
- It will give PSPs enough time, in most cases, to have completed investigation of scams notified during the period, to have made reimbursement decisions and to have identified sums to be repatriated.
- It will give us enough time to ensure that appropriate collation, review and queries are undertaken on the data ahead of publication.
- It is proportionate in terms of requirements on PSPs (such as the cost required to collate data and verify it with receiving PSPs).

4.36 The proposed timetable will provide PSPs with adequate time to address, before data is published, any new vulnerabilities to scams that they identify during the reporting period. We want to avoid potential to aid scammers, and welcome evidenced views on the implications of our proposed timetable.

Question:

12. Do you have comments on the proposed reporting period and timing for publication of data comparisons?

Data reporting and assurance

4.37 We propose to require directed PSPs to report complete and accurate data required under Measure 1 to us by a specified deadline following the end of each reporting period. Further details are set in Box 4.

Box 4: Data reporting and assurance

We propose:

- that the deadline for submitting data to us is three months after the end of the reporting period, and welcome views on this;
- that directed PSPs should give each relevant receiving PSP adequate opportunity to review the Metric C data related to that receiving PSP. The directed PSPs will be required to adjust the data as appropriate in light of comments received, and explain to the receiving PSPs (and the PSR) how they have taken account of any comments; and
- that each directed PSP's Chief Financial Officer, or an equivalent or more senior executive, should attest to us in writing that the data it submits to us is complete and accurate and prepared in accordance with our requirements. This will be an effective and proportionate approach to assuring data quality, noting our general powers for investigation and enforcement in relation to suspected non-compliance with our directions.

4.38 Timely decisions on reimbursement are important for minimising distress to victims. We expect PSPs to complete investigation and decision-making on cases notified to them in the reporting period, in time to include the relevant data in Measure 1 published comparisons. However, we recognise that, for a small number of exceptional cases in each period, data may not be final and adjustments may need to be included in reporting for the following period.

4.39 After the data is submitted to us, we will ensure it is reviewed and prepared for publishing comparisons. UK Finance currently plays a key role in collecting, collating, cleaning, cross-checking and querying data reported by Code PSPs (which is subsequently published in aggregate). We may ask UK Finance to help us in a similar way in relation to Measure 1 reporting, at least at the outset. Directed PSPs would remain legally responsible to us for the completeness and accuracy of their reported data. We will specify the data to be provided to us and agree with UK Finance the approach it takes in helping us. We will set out our requirements in the direction we propose to issue, and we also expect to issue guidance as required.

Questions:

13. Do you have comments on the proposed timetable for reporting data to the PSR?

14. Do you have comments on the proposed approach to quality assurance of the data?

Trialling measure 1

4.40 We propose to implement a trial run of Measure 1 data reporting and presentation (without publication), on a voluntary basis prior to us issuing our direction, to help refine processes.

4.41 Such a test run could be started quickly, using participants' existing data with agreement, and the results potentially considered, alongside feedback on this consultation and the draft direction, in formulating our final policy. As part of the trial run, we could enable each participant to see how they compare with anonymised data from the other participants, giving them the chance to challenge the comparisons or review their own data if they consider the comparisons contain errors. This could also enable participants to begin to take any actions in response to their trial run performance.

4.42 We see our Measure 1 direction as ideally having a finite life, depending on its effectiveness in reducing consumer losses from APP scams and on potential developments such as securing mandatory protection of APP scam victims. We do not propose to include a time limit in the direction because it is uncertain how long Measure 1 will be required. We propose to keep under review how performance reported under Measure 1 evolves over time. Our views on the effectiveness of Measure 1 will inform our decisions on roll-out to more PSPs over time.

Question:

15. Do you have comments on our proposals for trialling and reviewing Measure 1?

Proportionality and cost–benefit analysis

4.43 Our proposals for taking forward Measure 1 are proportionate in relation to their expected contribution to our objectives of preventing scams and ensuring customers are appropriately reimbursed.

4.44 Our cost-benefit analysis of the requirements proposed for Measure 1 is set out in Annex 1 to this paper. This sets out our assessment of a number of issues that are also relevant to proportionality.

4.45 As explained in Chapters 2 and 3, APP scams continue to grow, and there are problems with the current framework. APP scams can have a devastating effect on victims. Measures to incentivise better prevention of scams, and reimbursement in appropriate cases, are therefore of great importance in protecting consumers and maintaining confidence in payments systems.

4.46 We have set out how we expect Measure 1 to contribute to these objectives. We consider it will lead to reputational incentives, by raising awareness of PSPs' performance among a range of stakeholders and with PSPs' boards. We expect these reputational incentives to be strong, given the high public prominence of concerns about – and the increasing prevalence of – APP scams. PSPs have scope to respond to these incentives both in their approaches to reimbursing consumers and by taking further steps to prevent scams including, for example, implementing the sharing of standardised risk data (discussed in the next chapter).

4.47 In developing our proposals, we have taken account of the need to ensure they are proportionate. Our judgements are discussed in this consultation and include the following:

- The proposed scope of payments included in Measure 1 is limited to Faster Payments because the vast majority of APP scam payments are made over the Faster Payments system. We consider this provides Measure 1 with sufficient scope to achieve our objectives. At the same time, covering a smaller sub-set of payments would reduce the relevance to some consumers of the information PSPs must publish and weaken the reputational incentive on PSPs.

- The number of PSPs we propose to direct is necessary to cover all those PSPs enabling substantial numbers of consumers to make payments over Faster Payments, and sufficient to include the vast majority of payments and APP scams.

- By requiring data on receiving PSPs only from directed PSPs, we can collect data on a large number of APP scams without having to direct a potentially large number of receiving banks. It also enables us to publish comparisons of receiving banks covering the vast majority of payments. Requiring directed banks to share the relevant data with receiving banks, for their review, creates a small additional burden for both sending and receiving PSPs but is necessary to help ensure accurate data and a process that is fair to receiving PSPs.

- It is our view that any additional costs and burden on directed PSPs, or on other PSPs about which information may be published under Measure 1, will be relatively small and are outweighed by the importance of action to reduce the devastating effects of APP scams. We have, in particular, sought to design Measure 1 to build on information-gathering processes that PSPs already undertake, or are likely already to undertake.

4.48 We will continue to consider the proportionality of Measure 1 as we develop it further.

Question:

16. Do you have comments on our CBA for Measure 1?

5 Improving intelligence against fraud

We asked for views on a suggestion for standardised risk data to help support the identification of potential scams and enable PSPs to take action to prevent fraud. Since the call for views, an industry working group has been set up to look into what data could be shared to help prevent APP scams, and how this could best be done.

We welcome the action that is being taken to agree better ways to share information. We want to see PSPs develop new processes to prevent scams from happening. To ensure that proposals are taken forward in a timely manner, we will ask industry to develop a plan that will lead to concrete proposals, and associated rules and standards being delivered.

Industry initiatives

5.1 Fraud tools and risk-identification measures and processes exist within many PSPs. However, these measures are not common amongst PSPs. While PSPs may have information about the risk of a transaction, this information is not usually shared between the PSPs within the transaction. Greater sharing of standardised information and data would help support the identification of potential scams, and could enable the PSP to take action to prevent fraud.

5.2 A number of PSPs, along with UK Finance and Pay.UK have initiated an industry group (the Joint Working Group) to assess the specific information that could be shared. This group is looking to identify:

- the data it would be beneficial to share.
- the best way to share the data – for example, between PSPs when the payment relationship is first set up or as part of the payment itself.

5.3 The Joint Working Group aims to have high-level proposals on these points by the end of H1 2022. After this, we expect that this work will need to be taken forward by Pay.UK in producing the detailed rules and standards either through the Faster Payments system rules and standards, the Confirmation of Payee rules and standards or another set of rules and standards. PSPs would also likely need to make changes in order to be able to implement it.

5.4 The PSR has been invited to attend the Joint Working Group as an observer.

What we'll do

5.5 We welcome industry organising the Joint Working Group, and its efforts to find workable solutions to sharing information in a timely manner in order to prevent fraud. We are comfortable that this group is making progress and its aims align with our objectives for Measure 2.

5.6 We intend to ask the group to develop a plan of outcomes and timelines, and we will also ask it to report back to us on progress, as well as to consider wider communications to relevant stakeholders.

5.7 We will leave the technical design to the Joint Working Group, but the rules and standards must allow PSPs to gain additional information from each other that can lead to better detection and fraud protection. We also want to ensure that all PSPs and their customers can benefit from this measure, so any solution needs to be able to be adopted by a wide range of PSPs.

5.8 Further consideration will need to be given to the role of Pay.UK in developing rules and standards, as well as to how best to ensure PSPs adopt the relevant services thereafter.

5.9 We will also monitor other developments that may lead to the prevention of some types of APP scams, and understand the role the PSR should play in respect of widespread adoption if these are considered beneficial for preventing scams. Examples include: the Request to Pay (RtP) service that provides a secure messaging layer between billers and payers that could prevent some types of scam being initiated; and the Biller Update Service where PSPs pre-populate known biller accounts in digital payment channels to avoid being tricked into paying a bill into a scammers account. Some respondents to our Confirmation of Payee call for views mentioned that the upcoming extension of the service (through Phase 2) to capture secondary reference data would have the added benefit of collecting data in pre-payment messaging.[23]

5.10 We are confident that the industry will deliver credible outcomes. We will continue to monitor the Joint Working Group to ensure that they have credible plans and their work remains on track.

5.11 We will also monitor developments in the adoption of Request to Pay (RtP) services, improvements on the Biller Update Service and the use of secondary reference data in Confirmation of Payee.

Question:

17. Do you agree with our position on improving intelligence against fraud? We welcome any further comments from stakeholders about this work.

23 https://www.psr.org.uk/media/ktonkca3/psr-rp21-1-confirmation-of-payee-response-paper-oct-2021.pdf

6 Improving the protection of victims

While there are still problems with the approach to reimbursement by some CRM Code members, consumer outcomes under the Code have improved and we expect them to continue to do so.

This chapter focuses on a related issue – the currently limited coverage of the CRM Code, due to its voluntary basis.

Victims should be reimbursed, and so we develop two further options from our call for views paper:

- Requiring Pay.UK to change Faster Payments scheme rules to require reimbursement for all APP scam victims who have exercised sufficient caution.
- Requiring Pay.UK to incorporate into scheme rules a requirement for PSPs to sign up to a PSR-approved code.

We look at the pros and cons of the two options and ask for comments on these.

We believe that reimbursement of scam victims should be made mandatory. While there could be issues with imposing this at present, we are continuing to look at what we could currently achieve, including how we could best use our existing powers.

Issues with the CRM Code

6.1 In Chapter 2, we summarised concerns with customer outcomes under the CRM Code that were raised by respondents to our call for views. However, we have observed recent improvements in outcomes and in the way the Code is being implemented that should result in outcomes continuing to improve.

Addressing the Code's issues

6.2 The LSB and the Financial Ombudsman have both noted improvement over the past year in the performance of PSPs in relation to the Code. They have also set out steps in order to achieve further improvement:

- In January 2021, the LSB identified areas for improvement in the application of the Code by signatories. They also said that they had seen evidence that, when applied correctly, the Code provides significant protection for customers.[24]
- The LSB has provided clear and specific feedback to PSPs on the action they need to take to comply fully with the requirements of the Code, in reimbursement decisions, effective warnings during scams, and taking account of vulnerability.[25]
- The LSB has reinforced this message by writing to the Chief Executive of each PSP concerned, setting out their expectations of the steps that PSPs should take to ensure compliance with the Code, with deadlines.
- The Ombudsman shared the LSB's concerns about Code PSPs' reimbursement decisions and effective warnings.[26] We understand, anecdotally, that PSPs' performance on the latter has been improving, with PSPs considering the findings in appeal cases adjudicated by the Ombudsman leading to improvements in case handling.
- The Ombudsman has also published case studies on its website[27], providing guidance on how PSPs can improve their performance. This is a positive step, although we recognise that PSPs asked for more guidance of this sort to help them improve how they deal with victims.
- The developments above suggest that consumer outcomes under the Code are likely to continue improving. Two bodies are actively holding Code signatories to account over their performance and are continuing to steer those PSPs towards improving. We expect the LSB and Ombudsman to continue working to make the Code requirements as clear as possible and to work with PSPs to address any compliance issues. Of course, if this doesn't continue, we will consider using our powers to improve the situation.

24 https://www.lendingstandardsboard.org.uk/review-of-the-crm-code-for-authorised-push-payment-app-scams-published-by-the-lsb/

25 https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/06/CRM-Review-R21c-Follow-Up-Summary-Report.pdf

26 https://www.financial-ombudsman.org.uk/files/289009/2020-10-02-LSB-CRM-Code-Review-Financial-Ombudsman-Service-Response.pdf

27 https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams

Broadening protection

6.3 The nine current Code signatories account for the vast majority of payments made by relevant customers over Faster Payments (>80%). However, a number of smaller PSPs are not signatories. We are aware that there are barriers to some PSPs signing up to the CRM Code, which the LSB has a programme of work to address. However, there are also PSPs who could sign up to the CRM Code, or offer equivalent protections to customers, but have chosen not to. This points to the need to move from a system where victims rely on the commercial decisions of some PSPs to one where minimum standards of protection are made mandatory.

6.4 We want to ensure that all customers benefit from the same level of protection irrespective of their choice of PSP. This is important for trust in the system and to ensure there is a level playing field for PSPs. Scammers are also taking advantage of differences in protection by using non-Code (and non-CoP) banks for their receiving accounts. Both the options we put forward in our call for views – 3A and 3B – would address this issue by requiring PSPs to provide a minimum level of protection for their customers. As we have previously highlighted, there could be challenges with implementing either option at present, but we welcome the recent announcement from the Economic Secretary to the Treasury confirming that the Government will legislate to address any barriers to regulatory action at the earliest opportunity.

6.5 Since the call for views, we have been developing more detail of how both options could work in practice. This includes consideration of how best to implement the options, in light of any changes in the legislation, and other analysis – for example, on the possibility of directing participants as an alternative to requiring a payment system operator to change the rules of a payment system. We will explore this possibility and may include it in our consultation on the proposed way ahead, once we have more certainty about the timing and nature of legislative changes.

Pros and cons of the options

6.6 **We have identified two ways in which the PSR could ensure that reimbursement protections are available to customers irrespective of their choice of PSP.**

Option 3A

6.7 Requiring Pay.UK to incorporate into scheme rules an obligation for members to reimburse APP scam victims who have exercised sufficient caution

6.8 The rule could require reimbursement for all victims (subject to exceptions such as first-party fraud and other circumstances where the customer did not act appropriately).[28] The Ombudsman would still adjudicate on appeals from victims in individual cases. Compliance with the rule would have to be enforced, as are all Faster Payments and Bacs Direct Credit scheme rules, by Pay.UK, as the system operator.

6.9 This option would make the reimbursement elements of the CRM Code redundant in relation to Faster Payments. However, there are other elements to the Code – covering things such as case-handling, communications and deadlines – that could be continued if this option were to be adopted. All elements of the Code would still apply to CHAPS and on-us payments.

6.10 We set out these options previously in our call for views, but in light of the responses we received we are setting out our current views of their pros and cons to help inform our thinking:

Pros

6.11 The customers of all scheme participants would be covered, and we would expect the requirement to filter down to indirect participants through contracts with sponsor banks (as is currently the case with other Faster Payments rules).

6.12 This option also separates the issue of mandatory reimbursement from all other aspects of the existing Code, and would not require all the other aspects of the Code to be adapted to apply to all business models.

28 There are a number of options for what the rule could include – for example, elements of the existing CRM Code could be used, where appropriate. In relation to APP scams, first-party fraud is the term used to describe a scenario where the alleged victim is willingly part of the fraud (for example pretending that they have been scammed when they moved funds to someone they know).

Cons

6.13 The APP scam system rules would be administered by Pay.UK. We would need to consider how well equipped Pay.UK is to undertake this role.[29]

6.14 In order to be practicable for use in scheme rules, this option would have to have a much tighter definition of liability than that currently in the CRM Code, which would mean more liability falling on PSPs. Given that we have seen no evidence that the balance of consumer-PSP liability is wrong, this is recorded as an additional cost of this approach.

6.15 Relative to Option 3B, 3A would lead to a larger role for Pay.UK and could require it to take on new tasks. This may lead to greater transition costs, due to the further changes needed relative to the current situation. This is discussed in more detail below.

Option 3B

6.16 **Formalise the CRM Code by requiring Pay.UK to incorporate into scheme rules a requirement for PSPs to sign up to a PSR-approved code.**

6.17 For a code to be approved for this purpose, it would need to meet certain minimum requirements. This provides an opportunity to ensure that such a code would have ways to secure compliance and/or could be accompanied by requirements on PSPs to demonstrate a high level of compliance. The assessment of this could fall to the Code administrator. This may entail additional costs relative to the current situation.

6.18 If a PSP did not sign up to an approved code or is unable to demonstrate a high level of compliance, the default would be a requirement that they reimburse all victims of APP scams, subject only to very limited exceptions, such as evidence of first-party fraud.

What would make an approved code?

6.19 Under this option, the PSR would set out the criteria that we would require a PSR-approved code to fulfil. While we will not give an exhaustive list here, a Code would have to be highly likely to lead to the following things:

- by strengthening the requirement on sending and receiving PSPs **Reducing APP scam fraud** to improve fraud detection and prevention controls.
- **Broadening protection** through widespread uptake amongst PSPs, including smaller PSPs.
- **Customer education** preventing more scams through improved risk warnings and customer knowledge and awareness of APP scams.

29 This could form part of the PSR's strategic priority to ensure the future governance of the UK's interbank payment systems supports innovation and competition in payments.

- The Code has a **governance structure** that will result in high compliance, and consistent interpretation, including the withdrawal membership for failure to compl Improved outcomes for customers y on a systematic basis with code obligations.

- **Improved outcomes for customers**, including those considered more susceptible to APP scams.

Pros

- As with option 3A, this option would extend coverage to all PSPs – either through code membership or the reimbursement requirement.

- A modified version of the CRM Code could become an approved code, building on the existing code as well as the roles of the LSB and the Ombudsman, although this option would be sufficiently flexible that it does not necessarily have to be the case.

- This option would likely bolster the authority of the LSB and help to ensure compliance with the code.

Cons

- In order to sign up to an approved code, PSPs would have to be able to fulfil all its requirements, meaning it could take time for a code to be put together that a high number of/all PSPs would be able to sign up to. Given the likely timetable for any new rule, we assume that these issues could be addressed before the rule would take effect.

Roles under the two options

6.20 Our thinking is that the roles of the bodies currently involved in the CRM Code would differ between the two options under Measure 3.

Table 5: Roles under Measure 3

	Option 3A	Option 3B
Pay.UK	Pay.UK would administer and enforce the reimbursement rule (that might require changes to Pay.UK's current governance).	Pay.UK would administer and enforce the reimbursement rule default for any PSPs that are unable to demonstrate a high level of compliance with an approved code (that might require changes to Pay.UK's governance).

	Option 3A	Option 3B
LSB	The LSB could continue to administer the non-reimbursement elements of the CRM Code, if this was carried on as a voluntary agreement by PSPs.	If the CRM Code became an approved code, we would envisage the LSB in an administration and enforcement role for PSPs signing up to this code.
Financial Ombudsman	As there would still be some discretion for PSPs in the application of the reimbursement rule, the Ombudsman would still have a role as appeals body.	We envisage the Ombudsman continuing in its role as appeals body for those PSPs subscribing to a code under this option.
PSR	The PSR would monitor Pay.UK's implementation of the rule requirement into FPS rules, and its approach to monitoring and enforcing compliance with the rule.	The PSR would monitor Pay.UK's implementation of the rule requirement and approach to monitoring and enforcing compliance. The PSR would also monitor the performance of the LSB in enforcing an approved code.

6.21 The roles of these bodies could also vary further depending on the instrument used to implement whichever option was chosen.

Question:

18. Do you have any comments on our thinking on how the roles of the bodies currently involved in the CRM Code would differ between the two options under Measure 3?

Implementation issues

6.22 The current legislation prevents the PSR from directing PSPs to reimburse APP scam victims. However, if changes in the legislation were to happen that allowed the PSR more flexibility in this area, there could be two possible approaches:

- The PSR writes the rule change;
- The PSR requires the system operator to write rule changes to achieve specified outcomes.

6.23 We received very little comment on this in responses to our call for views, and views were balanced between the two options. We will continue to consider the most appropriate method of implementation and consult on our proposed approach.

Other ways of making progress

6.24 We welcome the recent announcement from the Economic Secretary to the Treasury confirming that the Government will legislate to address any barriers to regulatory action at the earliest opportunity.

6.25 As well as anticipating changes in the legislation to allow us to require reimbursement from victims' PSPs, and preparing to use, if appropriate, any new powers when they become available, we are continuing to look at what we could currently achieve before any legislative changes. This includes how we could best use our existing powers – for example looking at FPS scheme rules to understand how they compare to rules in other payment systems such as card schemes, looking at the balance of liability between sending and receiving PSPs to incentivise better fraud prevention and reimbursement outcomes, mandating further fraud prevention, or further enhancements to the CRM Code. On the latter of these, we will be exploring what enhancements could be carried out by the LSB.

6.26 We also believe there could be significant value in voluntary action by PSPs to improve outcomes for customers. As mentioned above, there is an industry working group on developing ways to share transaction risk data between PSPs.

6.27 By the same token, there are additional areas we would like to explore, including voluntary action by Pay.UK and PSPs. This could include further investment in the prevention of APP scams, such as in detection technology and fraud analytics, or implementing rules (for example, in Faster Payments) within the parameters of existing legislation. We know that a number of PSPs want to take these types of actions as a matter of priority but that coordination across the whole industry can be a challenge. We're also aware that Pay.UK has recently set up a programme of activity to explore what can be delivered to assist fraud detection and prevention. Therefore, in addition to exploring these options further in our own work, we will facilitate the coordination of industry in coming together to address this significant problem urgently. We will also work with other regulators to co-ordinate actions tackling APP fraud.

7 Next steps

7.1 Measures 1-3 are a package that we originally asked for views on. As discussed above there are various initiatives to ensure these measures achieve their impact and a number of questions we would appreciate views on. We are asking for feedback on the issues set out in this paper by 14 January 2022. We continue to welcome feedback from all stakeholders and interested parties, not only entities that we regulate.

7.2 You can provide feedback by emailing us at **appscams@psr.org.uk**. We would be grateful if you could provide your response in a Microsoft Word document (rather than, or as well as, a PDF).

7.3 We will make all non-confidential responses available for public inspection. If your submission includes confidential information, please also provide a non-confidential version suitable for publication.

7.4 In addition to the package of measures set out in this paper, we will continue to look at other ways of preventing APP scams and ways in which victims of APP scams could be reimbursed. This could likely include promoting the development of additional technical solutions (e.g. on customer fraud analytics); looking at ways the PSR, Pay.UK, and industry could implement rules (e.g. in Faster Payments) within the parameters of existing legislation; and wider adoption of existing measures e.g. Request to Pay and the Biller Update Service.[30]

7.5 We anticipate further interaction with industry in H1 2022 on whether these areas, or others, could lead us to a position where we are able to propose a further package of measures that would be effective in combatting the impact of APP scams. We will also work with other regulators to co-ordinate actions tackling APP fraud.

Timetable

Q1 2022	The PSR will consider the responses to this consultation and decide on its next steps.
H1 2022	The PSR will publish a policy statement, outlining the measures we intend to introduce to continue our programme of work to improve protection against APP scams.
H1 2022	The PSR will engage with industry on further initiatives to combat the impact of APP scams.

30 Confirmation of Payee (CoP) is a further measure but being addressed separately.

List of questions

Chapter 4: PSP data on APP scams

1. Do you have comments on our proposed data metrics?
2. Do you have comments on the proposed scope of payments included in Measure 1?
3. Do you have views on the scam value bands for Metric A data?
4. Do you have any comments on the draft direction at Annex 3?
5. Do you have comments on our proposal for which PSPs should initially be required to report and publish Measure 1 data?
6. Do you have views on how long it will take directed PSPs to put in place the necessary reporting systems?
7. Do you have comments on our proposal to allow PSPs to be voluntarily included in published data comparisons?
8. Do you have comments on how and where data comparisons between PSPs are published, including our proposals to compare PSPs at PSP group level?
9. Do you have views on the basis we use for determining which receiving PSPs are included in published Metric C comparisons?
10. Do you have comments on our proposal for the preparation and validation of information about receiving PSPs?
11. Do you have comments on how we specify where PSPs must publish the data on their websites?
12. Do you have comments on the proposed reporting period and timing for publication of data comparisons?
13. Do you have comments on the proposed timetable for reporting data to the PSR?
14. Do you have comments on the proposed approach to quality assurance of the data?
15. Do you have comments on our proposals for trialling and reviewing Measure 1?
16. Do you have comments on our CBA for Measure 1?

Chapter 5: Improving intelligence against fraud

17. Do you agree with our position on improving intelligence against fraud? We welcome any further comments from stakeholders about this work.

Chapter 6: Improving the protection of victims

18. Do you have any comments on our thinking on how the roles of the bodies currently involved in the CRM Code would differ between the two options under Measure 3?

Annex 1
Cost benefit analysis – information publication

1.1 As outlined in Chapter 4, we are proposing to require the 12 largest PSPs in the UK and the two largest banks in Northern Ireland outside those PSPs to report and publish a balanced scorecard of data comparisons on a six-monthly basis, setting out their performance in relation to APP scams. The outcomes we are ultimately seeking through this policy are to improve incentives on PSPs to prevent APP scams from happening in the first place and, where they do happen, to reimburse victims.

1.2 This annex contains our cost benefit analysis. We first set out the ways in which we expect the policy to affect customer and PSP behaviour, and ultimately improve outcomes (the causal chain), before providing our initial assessment of the most significant impacts of our proposal. We have not sought to quantify all of these impacts at this stage – given that in some cases it might not be obvious how the effects will manifest themselves and, therefore, how they can be quantified with precision. We note, however, that even where some effects cannot be quantified with precision, this does not necessarily mean that they are immaterial. We have relied on indicative evidence to carefully weigh these multiple dimensions and reach an overall judgement about the likely impact of the policy.

1.3 We welcome stakeholder views on our approach and the significant impacts we have identified, including any evidenced views on their likely relative magnitude.

How the policy could improve outcomes

1.4 There are two main mechanisms through which the publication of a balanced scorecard of data could impact the level of APP scam-related fraud and reimbursement:

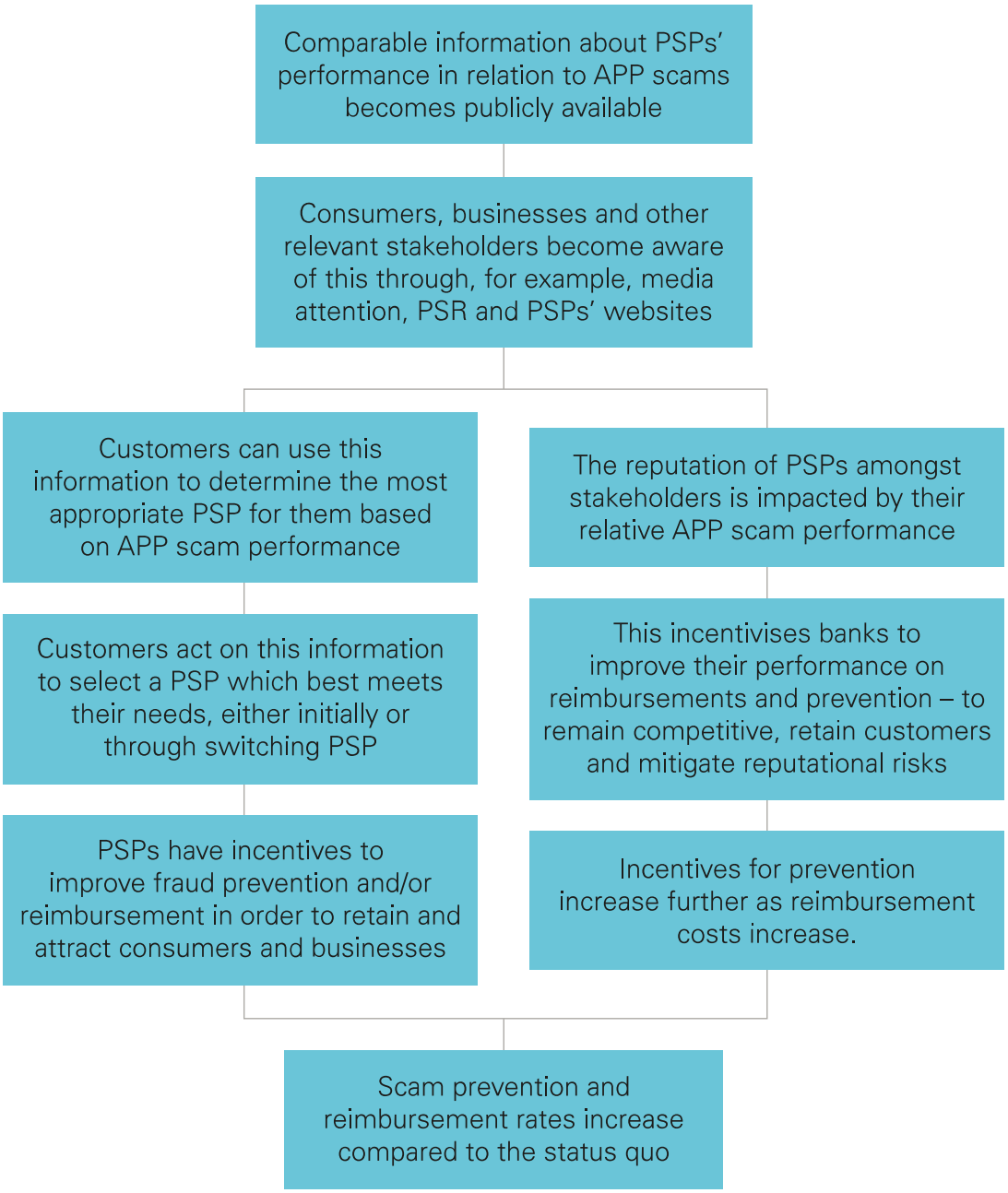
- First, customers may factor these metrics into their decisions when selecting a PSP. This could help inform their initial choice of PSP as well as potentially impacting some marginal customers' decisions when considering their switching options. Therefore, it could potentially enable these users to select a PSP which best meets their needs regarding APP scam performance, and this could also drive incentives on PSPs to improve their performance to attract and retain more customers.

- Second, greater public awareness of PSPs' relative performance in relation to APP scams is likely to have an impact on their reputation with a range of key stakeholders including government, politicians, investors, journalists, consumer groups, employees and regulators, as well as customers. We expect these reputational incentives to be strong, given the high public prominence of concerns about – and the increasing prevalence of – APP scams. This is likely to provide PSPs with an incentive to improve their relative performance – independent of any direct reaction from their customers, in terms of customer switching or new customers choosing other PSPs for their first current account. These indirect effects would be felt through the impact on reputation and 'brand value' of the PSPs in question. Ultimately, these effects are also likely to influence consumer decisions.

1.5 We consider that the policy is likely to have its greatest impact through the second of these mechanisms. This is because, as highlighted by previous work in this area, demand-side pressure in retail banking is likely to be weak.[31] This means that we would expect many consumers not to access this information in the first place. Even for those who do, we would expect that some may be unable to identify the most appropriate PSP for them or act to select the most appropriate PSP for them, and/or that it would be only one of a number of factors affecting their decision making. In contrast, we would expect reputational effects from the reactions of more informed stakeholders, like government, investors, journalists and consumer groups, as well as PSPs' boards, to be more effective in targeting those PSPs that most need to improve their performance.

31 See, for example, the CMA's Retail banking market investigation report, paragraphs 64-85.

Figure 6: Causal Chain of Measure 1



The baseline

1.6 We have analysed the impacts of the policy against a baseline, or 'counterfactual', scenario. The starting point for our baseline is that PSPs will continue taking some action to prevent APP scams and reimburse victims who have exercised sufficient caution.

- Nine of the 14 PSPs that we are proposing to direct are currently signatories to the CRM Code, under which they have existing obligations regarding preventing APP scams and protecting victims.[32]
- Existing regulatory requirements, and likely future requirements, mean that PSPs have incentives to prevent scams. For example, PSPs have existing FCA requirements to consider the needs of their customers.
- As the reimbursement of APP scams represents a cost to PSPs, we would also expect that they would continue to face commercial pressure to prevent scams. This incentive depends upon the approach taken to reimbursement.

1.7 As part of our baseline, we also consider that PSPs already conduct analysis on their APP scam performance to inform their internal decision making. As above, 9 of the 14 PSPs which we are proposing to direct are currently signatories to the CRM Code, so are already collecting and submitting the relevant data. We also understand that most PSPs already regularly submit data on APP scams to industry bodies and regulators and assume this would continue in the baseline. Our analysis is therefore focused on the incremental costs and benefits that will materialise in addition to those already occurred due to the PSPs' current actions.

32 We note that a tenth PSP, Virgin Money (owner of Clydesdale Bank) signed up to the Code in July 2021 and will become a fully registered member within a year of that date – see the LSB website.

Summary of our assessment of the impacts

1.8 Table 7 summarises our initial assessment of the likely costs and benefits of the policy relative to the baseline, and the likely magnitude of these.

Table 7: Impacts arising from achieving greater transparency

Benefits		Costs	
Type	**Magnitude**	**Type**	**Magnitude**
Consumers able to select a PSP which best meets their needs in respect of APP scam performance (direct benefit)	Low	Collating and reporting high-quality data (direct cost)	Low
Better prevention of APP scams (indirect benefit)	High	Improving investment on fraud prevention (indirect cost)	Medium
Improved reimbursement rates for APP scam victims who have exercised sufficient caution (indirect benefit)	High	Unintended facilitation of fraud (indirect cost)	Low
		Potential exclusion of customers, who may be vulnerable, in accessing current accounts (indirect cost)	Low
		Incorrect reputational damage to PSPs (indirect cost)	Low

1.9 Considering these impacts in the round, we consider that the benefits of publishing the three proposed metrics on Measure 1 are likely to significantly outweigh the costs. In undertaking this assessment, we have sought to account for the likely timeframe in which these impacts will be realised. We recognise that some of these impacts, potentially the largest costs, may occur immediately and materialise mostly in the beginning of the policy, such as the cost to some smaller PSPs of creating the required mechanisms of reporting and publishing this data. On the other hand, most benefits may take some time to fully materialise but we envisage that they will continue throughout the periods – for example the better prevention of APP scams.

Analysis of the impacts

Analysis of the benefits

1.10 **Consumers are able to select a PSP which best meets their needs in respect of APP scam performance (direct benefit).** In its 2016 Market Investigation into retail banking, the CMA found significant demand-side barriers to consumers accessing, assessing and acting on information when selecting a personal current account. For example, switching rates for PCAs was about 3% a year, and many of those consumers selected accounts based on better interest rates, customer service or branch availability.[33] Whilst initiatives since then may have had some effect on switching behaviour, we consider that this is unlikely to have changed significantly. However, if consumers do want to take into account PSPs' fraud prevention rates or reimbursement rates when deciding on which PSP to bank with, we want information to be available to allow them to do so. Even if a small number of consumers decide to act on the information and switch to a PSP with higher fraud prevention rates and/or reimbursement rates, that would represent a direct benefit to consumers from the greater transparency. Given the modest number of consumers we believe will act upon this information, we would not anticipate that the competition effects will be of the magnitude to incentivise PSPs to change behaviour but we do believe that there will be some overall benefits from the consumers who do switch to PSPs that have higher reimbursement rates and/or better fraud prevention rates.

1.11 **Better prevention of APP scams (indirect benefit).** We consider that the overall magnitude of this effect is likely to be high. Reported losses from APP scams have been rising, even before the COVID pandemic provided new opportunities for scammers and new vulnerabilities amongst consumers, with a 29% increase in the value of losses due to APP scam fraud between 2018 and 2019.[34] In the first half of 2021, losses from APP scams totalled £355.3 million, an increase of 71% compared to the same period the previous year.[35] This is likely to be an underestimate due to unreported fraud. In the first half of 2021, the PSPs we are proposing to direct account for over 95% of FPS transactions, and the vast majority of APP scam payments sent over Faster Payments (as reported by UK Finance members). We also note that many cases of APP fraud involve individuals being scammed out of life-changing sums of money, with this ending up in the hands of criminals instead. Moreover, consumers face psychological costs associated with losing their savings to fraudsters. Even if they are fully reimbursed (weeks or months later), they will still suffer a cost for losing the money in the first place and will face the stress and anxiety of not knowing if and when they will be reimbursed. Preventing scams from happening will instead mitigate these issues. Therefore, we consider that even a modest increase in fraud prevention as a result of this policy is likely to have material benefits for the individuals concerned.

33 GfK NOP survey report for the CMA's Retail banking market investigation, Figure 38.

34 See UK Finance, Fraud – the facts 2020, page 46.

35 See UK Finance 2021 Half year fraud update.

1.12 **Improved reimbursement rates for APP scam victims who have exercised sufficient caution (indirect benefit).** We consider that this effect is also likely to be high. Whilst reimbursement rates among CRM-member PSPs is generally higher than it was before the CRM Code came into force, we still consider there is scope for improvement. We have heard anecdotal concerns about the consistency with which the code is being applied which is mirrored by feedback from the LSB and the Financial Ombudsman. The large variation in reimbursement rates among code signatories suggests that there is significant scope for some PSPs to improve their rates. For example, in Q4 2020, among the nine signatories the rate of reimbursement and repatriation ranged from around 30% to 76% of APP losses assessed under the CRM Code. Large discrepancies were also reflected across the whole of 2020, with annual averages for PSPs ranging from 18% to 64%.[36]

1.13 The publication of the three proposed metrics will also provide PSPs that have not signed up to the CRM Code, but also PSPs in receipt of APP scams included in the published data, with an additional incentive to improve their reimbursement rates. As outlined above, APP scam volumes have been increasing over time, with victims often losing life-changing sums of money. This means that any improvement in reimbursement rate would likely have a significant impact to victims, both in terms of recovering the lost amounts but also in increasing trust in the payment system for consumers more generally through an increase in their confidence that they will be able to recover any money lost where they have exercised sufficient caution.

Analysis of the costs

1.14 **Collating and reporting high-quality data (direct cost).** We consider that the directed PSPs will incur costs with providing this data – including extracting, quality assuring, transferring and responding to any queries on the data. We believe that the magnitude of these costs is likely to be low for a number of reasons:

- We believe it is likely that these PSPs already analyse data on their APP scam performance to inform their internal decision making. Moreover, we understand that for most of these PSPs, broadly similar data is already made available to industry bodies and regulators. We appreciate that the exact metrics we are proposing will differ in some ways to the data already collected and provided, but think that the incremental costs are likely to be low given processes already in place for doing this.

- We understand that the requirement for a CFO, or equivalent, to assure the quality of data being provided is likely to have costs associated with this. However, we feel that this is necessary to ensure the data is high quality and not misleading. We also note that we would expect that senior management within each PSP would want to understand their relative APP scam performance. We would also expect this cost – and the costs more generally of collating and reporting the data – to reduce over time as PSPs become familiar with the reporting requirements. As above, the incremental costs – over and above what PSPs are already doing on this issue – are likely to be small.

36 See our Call for Views, Figure 4.

- We believe that directing the proposed PSPs is most proportionate. As set out above, they broadly have the required mechanisms in place and therefore we believe the incremental costs they might face will be minimal.

1.15 **Improving investment on fraud prevention (indirect cost).** As outlined above, we understand that PSPs have existing programmes to promote fraud prevention and consumer education. We would expect the directed PSPs to have incentives to increase prevention as a result of this policy but expect this incremental cost to be relatively modest given they would be building on existing initiatives. Fraud prevention would also realise further benefits both to the PSP, industry and society more generally, to the extent that it prevents frauds from happening in the first place.

1.16 **Unintended facilitation of fraud (indirect cost).** We understand that, in theory, there is a concern that any data published about a PSP's APP scam performance may help scammers target PSPs with potential weaknesses in their systems. We believe that this risk – and therefore cost – is likely to be low. We consider that data suggesting a PSP has previously been disproportionately targeted by scammers is unlikely to reveal new information to scammers. In addition, under the timelines proposed in the policy, PSPs would have time to address any weaknesses in their systems before each wave of data is published.

1.17 **Potential exclusion of customers, who may be vulnerable, in accessing current accounts (indirect cost).** We have considered the risk that – in trying to improve their APP scam performance – PSPs may apply stricter criteria when deciding whether to allow a customer to open a current account. This could lead to some groups of customers, who potentially are more likely to exhibit characteristics of vulnerability, struggling to open an account. We consider that this risk is likely to be low in practice given wider requirements on PSPs to protect vulnerable consumers and promote inclusion. We also consider that whilst, in theory, applying stricter criteria may improve a PSP's performance on a single metric, it may not materially improve their overall performance across the balanced scorecard.

1.18 Incorrect reputational damage to PSPs (indirect cost). We note that there is a risk that stakeholders may make incorrect inferences about a PSP's performance from the available information – for example, if they make assessments based on just one metric, rather than the balanced scorecard. This could lead to some PSPs facing unwarranted reputational damage. We consider the likely magnitude of this to be low in practice, as we believe that this can be minimised through how the data is presented on the PSPs' and the PSR's websites. The presentation of these metrics is something we are considering carefully as we develop the policy.

Annex 2
Public sector equality assessment

In line with our public sector equality duty under the Equality Act, we must assess the likely equality impacts and rationale for any measures we propose and consult on.

In this chapter we explore further the impacts we believe the measures we are considering (and their implementation) will have, including on those with relevant protected characteristics, and we ask for comments and evidence to support us in carrying out our assessment.

The purpose of our PSED assessment

2.1 In developing the three measures discussed in this paper, we have considered the matters set out in section 149 of the Equality Act 2010 (the public sector equality duty), particularly the impact of our proposed direction on people with protected characteristics. We have also considered those matters in developing the draft direction implementing Measure 1, including when deciding whether to propose a direction, who to direct and what should be in the direction.

2.2 Although the measures vary in approach, they have mutually supporting purposes. Measures 1 and 3 both aim to incentivise PSPs to prevent APP scams. Measure 1 would provide reputational incentives both to prevent APP scams and to reimburse customers affected by APP scams, where they have exercised sufficient caution. Measure 3 would aim to improve reimbursement of APP scams by increasing the scope of PSPs included under a reimbursement requirement. This should incentivise greater prevention of APP scams by PSPs. Measure 2 is intended to assist PSPs in preventing APP scams. Given the overlapping, and mutually supporting, purposes of the three measures we consider each of them has similar equality impacts. We have therefore assessed them as a package.

2.3 Overall, we currently believe that the measures we are proposing should have a positive impact on all those who use payment systems, including those with protected characteristics, because the measures should reduce the risk of APP scams and consumers becoming a victim of an APP scam.

Risks associated with our proposals

2.4 We are mindful that the proposed measures could present a greater risk of poor outcomes to some consumers with protected characteristics as they may be perceived as being more likely to being vulnerable to APP scams. This may include the elderly, people with serious mental health conditions and may also include some consumers with attributes linked to a protected characteristic, such as those who do not speak English as a first language. Our decision making on whether to implement the proposed measures will therefore consider issues around the risk of the:

- Reduction or denial of banking or payment services offered to customers with these protected characteristics, because they may be perceived by PSPs as being more at risk of falling victim to APP scams. Under the measures set out in this consultation, PSPs will be incentivised to reduce the incidence of APP scams among their customers. One response to this might be for PSPs to try to reduce this risk by either reducing or stopping the payment or banking services available to those among their customers regarded as more at risk of falling victim to APP scams.

- Reduction or ceasing of use of banking or payment services by customers with these protected characteristics because their awareness and/or their reluctance to use some payment methods, might increase due to the increased availability of APP scam figures or increased warning activity by their PSPs, resulting from their increased APP scam prevention activity.

2.5 Slowing of some payments or payment services for all customers, including those with protected characteristics, because some PSPs, due to increased incentives to prevent APP scams, will slow some payments or payment services for all customers, including people with these protected characteristics, while they investigate possible fraud. There is the possibility that this might affect people with these protected characteristics more than other customers, given that they may be perceived as more at risk of scams.

2.6 To the extent that they might result in PSPs delaying a small proportion of payments, we believe that the small amount of 'friction' being added to payments would be proportionate for increased detection of APP scams and resulting protection from this fraud.

2.7 To mitigate these potential adverse impacts, we will make it clear to PSPs in any decision to implement the proposed measures to incentivise them to improve their prevention of APP scams that they must ensure that the needs of people with disabilities, the elderly and other groups considered to be vulnerable are met. For example, we will make it clear that customers more at risk of being victims should not be refused or denied payment services to 'improve' the APP scam figures to be published under Measure 1. Similarly, any transaction risk information shared under Measure 2 should not be used to identify higher risk customers with a view to denying or refusing them payment services. We also expect PSPs to continue to treat all prospective customers equally, regardless of their vulnerability to APP scams.

2.8 We welcome comments on our equality impact assessment.

Annex 3
Draft Direction

DRAFT Specific Direction X requiring publication of information relating to authorised push payment scams

Specific Direction (Publication of APP scams information)

November 2021

Specific Direction (Publication of APP scams information)

1 Recitals

Whereas:

1.1 Authorised push payment (APP) scams occur when a fraudster tricks someone into sending money to an account that the payer believes is legitimate but is in fact under the control of the fraudster.

1.2 Those who make payments using payment systems have an interest in being protected against the risk of APP scams.

1.3 The Faster Payments Scheme is a push payment system used for sending money between different PSPs in the United Kingdom. More than 90% of APP scams happen over Faster Payments. Therefore, a significant reduction in APP scam payments across Faster Payments will significantly reduce the number of APP scam payments overall.

1.4 The Payment Systems Regulator (PSR) considers that increasing transparency of data about APP scams involving payment services providers (PSPs) executing payments across Faster Payments, and about how PSPs respond to those APP scams, will give PSPs whose information is published a greater incentive to prevent APP scams and to reimburse consumers where appropriate.

1.5 This direction is addressed to specified PSPs in the 12 largest UK banking groups, and the two largest independent banks in Northern Ireland, measured in terms of payments sent across Faster Payments. In the first half of 2021, these groups together accounted by volume for over 95% of Faster Payments transactions and the vast majority of APP scam payments sent over Faster Payments. By directing these PSPs, the PSR will cover the vast majority of APP scam payments over Faster Payments.

1.6 The PSR has decided to require the directed PSPs to provide information about APP scam payments they have sent to receiving PSPs within specified periods. The PSR will compile comparisons of the information relating to each directed PSP and certain receiving PSPs, and will require the directed PSPs to publish the comparisons periodically. The PSR will also publish the information about sending and receiving PSPs so that it is available in a single place.

2 Powers exercised and purpose

2.1 Faster Payments is designated by the Treasury under section 43 of the Financial Services (Banking Reform) Act 2013 (the Act) for the purposes of Part 5 of the Act.

2.2 The PSR makes this direction under section 54 (Regulatory and competition functions – directions) of the Act. In accordance with section 54(3)(c), this direction applies to persons of a specified description.

2.3 The purpose of this direction is to require directed PSPs to provide specified information to the PSR, and to publish comparisons prepared by the PSR using that information.

Direction

NOW the PSR gives the following specific direction to [directed parties]:

AIB Group (UK) Plc

Bank of Scotland plc

Barclays Bank UK plc

Barclays Bank plc

Clydesdale Bank plc

The Co-operative Bank plc

HSBC Bank plc

HSBC UK Bank plc

Lloyds Bank plc

Metro Bank plc

Monzo Bank Limited

National Westminster Bank plc

Nationwide Building Society

Northern Bank Limited

Royal Bank of Scotland plc

Santander UK plc

Starling Bank Limited

TSB Bank plc

Ulster Bank Limited

Virgin Money UK plc[37]

37 Bank of Scotland plc, and Lloyds Bank plc are part of the Lloyds Group; Barclays Bank UK plc and Barclays Bank plc are part of the Barclays Group; HSBC Bank plc and HSBC UK Bank plc are part of the HSBC Group; National Westminster Bank plc, Royal Bank of Scotland plc and Ulster Bank Limited are part of the Nat West Group; Santander UK plc is part of the Santander Group; Northern Bank Limited is a member of the Danske Bank Group; TSB Bank is part of the Sabadell group; Virgin Money UK plc and Clydesdale Bank plc are part of the Virgin Money UK Group.

3 General provisions

Scope of this direction

3.1 This direction applies in relation to payments, including APP scam payments, executed through Faster Payments.

Requirements for preparing and publishing information

3.2 A directed PSP must:

a. ensure any information it prepares or publishes under this direction is complete and accurate

b. comply with any requirements concerning the preparation, presentation or content of that information that the PSR notifies to it in writing from time to time, or that the PSR includes in any published guidance

3.3 Any such requirements may cover any matter the PSR considers necessary or appropriate, including:

a. the methodology for collecting or preparing information to be shared with the PSR or a PSP

b. the form a directed PSP must use to present information to the PSR or a PSP

c. the timing and manner of any publication required by this direction or by the PSR

d. how a directed PSP must break down information it shares or publishes, including displaying the information separately for different cases (such as different levels of loss arising from APP scam payments)

4 Key definitions

Definitions relating to APP scams

4.1 In this direction:

a. 'APP scam case' means a fraudulent act, or a fraudulent course of conduct, that leads to one or more APP scam payments

b. 'APP scam payment' means a payment that is executed by the sending PSP in accordance with an authorisation (within the meaning of regulation 67 of the

Payment Services Regulations 2017) given by its customer but where the customer is deceived into granting that authorisation as part of an APP scam, including because:

1. the payer intends to transfer the funds to a person other than the recipient but is deceived into transferring the funds to the recipient

2. the payer intends to transfer the funds to the recipient for purposes the payer believes are legitimate but which are in fact fraudulent

Publication months and related dates or periods

4.2 In this direction, in relation to a calendar year:

a. 'publication month' means each of the months mentioned in the first column of Table 1

b. the 'PSR reporting day' for a publication month is the day mentioned in the second column of Table 1, in the row for that publication month

c. the 'reporting period' for a publication month is the period specified in the third column of Table 1, in the row for that publication month

Table 1: publication months, PSR reporting days and reporting periods

1. Publication Month	2. PSR Reporting Day	3. Reporting Period
January	The first working day in October in the calendar year before the publication month.	The period from the beginning of January to the end of June in the calendar year before the publication month.
July	The first working day in April in the same calendar year as the publication month.	The period from the beginning of July to the end of December in the calendar year before the publication month.

5 Reporting periods, APP scam cases and APP scam payments

5.1 Any information about payments, APP scam cases or APP scam payments that a directed PSP provides to the PSR or another PSP under this direction in relation to a publication month must relate to the reporting period for that publication month.

5.2 Any information about payments, APP scam cases or APP scam payments published by a directed PSP under this direction in a publication month must relate to the reporting period for that publication month.

5.3 For the purposes of this direction:

a. a payment is deemed to be made in a reporting period if the payer's instruction to their PSP to make the payment is given in that reporting period

b. an APP scam case is deemed to occur wholly in a reporting period if in that reporting period

1. a payment resulting from that APP scam case is first reported as a potential APP scam payment to the sending PSP for the payment

2. the sending PSP for a payment resulting from that APP scam case identifies the payment as a potential APP scam payment

c. an APP scam payment is deemed to be made in a reporting period if in that reporting period:

1. the APP scam payment is first reported as a potential APP scam payment to the sending PSP for that APP scam payment

2. the sending PSP for that APP scam payment identifies the payment as a potential APP scam payment

6 Provision of information to the PSR to be prepared for publication

6.1 A directed PSP must provide the PSR with the information specified in paragraph 6.2 by the PSR reporting day for each publication month.

6.2 The information is:

a. in relation to APP scam cases or APP scam payments in which the directed PSP is the sending PSP:

1. the proportion by number of those APP scam cases in which the directed PSP's customer is not fully reimbursed by the directed PSP (whether using the directed PSP's own funds or recovered funds of its customer)

2. the proportion of total losses arising from those APP scam payments that is not reimbursed by the directed PSP (whether using the PSP's own funds or recovered funds of its customer)

3. the proportion of the total number of consumer payments the directed PSP sends that are APP scam payments

4. the total value of those APP scam payments that are consumer payments, as a proportion of the total value of consumer payments sent by the directed PSP

b. the name of each PSP the directed PSP makes one or more APP scam payments to (each an 'identified receiving PSP')

c. the total value of APP scam payments the directed PSP sends to each identified receiving PSP that are consumer payments (each an 'APP scam receipt total')

d. the total amount of funds forming part of the APP scam receipt total that each specified receiving PSP returns to the directed PSP (each a 'repatriation total')

e. the total value of consumer payments the directed PSP sends to each identified receiving PSP (each a 'consumer payment total')

7 Verification of receiving PSP information

7.1 For each publication month, a directed PSP must complete the steps set out in this section within 20 working days following the day on which the PSR provides the directed PSP with the information set out in paragraph 7.2.

7.2 The information mentioned in paragraph 7.1 is the names of the receiving PSPs that the PSR has determined must be included in information to be published under section 8 for that publication month (each a 'specified receiving PSP').

Notification of information to receiving PSPs

7.3 A directed PSP must give each specified receiving PSP:

a. the APP scam receipt total, repatriation total and consumer payment total for that specified receiving PSP (together the 'receiving-PSP information')

b. any other information the specified receiving PSP reasonably requires to assess the receiving-PSP information

7.4 A directed PSP must also give each specified receiving PSP a statement that:

a. the directed PSP has submitted the receiving-PSP information to the PSR to form the basis of information to be published during the relevant publication month by

   1. the PSR

   2. directed PSPs, under this direction

b. the specified receiving PSP may request further information it reasonably requires to assess the receiving-PSP information before the end of the period of five working days beginning on the day it receives the receiving-PSP information (the 'request period')

c. the specified receiving PSP may give the directed PSP comments on the receiving-PSP information, or the preparation of that information, to enable the directed PSP to determine whether it is appropriate to make any adjustments to the receiving-PSP information

d. any comments must be:

   1. provided before the end of the period of ten working days beginning on the day the specified receiving PSP receives the receiving-PSP information (the 'response period')

   2. supported by reasons and, so far as reasonably possible, evidence

Consideration of comments from receiving PSPs

7.5 A directed PSP must promptly:

a. respond to any request from a specified receiving PSP for further information in the request period

b. make any adjustments to the receiving-PSP information for a specified receiving PSP that are appropriate as a result of any comments (including the supporting reasons and evidence) received from that specified receiving PSP in the response period

c. provide that specified receiving PSP a reasoned written explanation of how it has taken account of each such comment

d. provide the PSR, for each specified receiving PSP, details of any adjustments made to the receiving-PSP information under this paragraph and a copy of the information provided under paragraph 7.5(c)

8 Publication of information provided by the PSR

8.1 A directed PSP must publish information in each publication month, on a day specified by the PSR, that is provided to it by the PSR and shows a comparison of:

a. for each specified receiving PSP, the aggregate of its APP scam receipt total net of its repatriation total for each directed PSP as a proportion of the aggregate of its consumer payment total for each directed PSP

b. for each directed PSP, each of the four categories of information listed in paragraph 6.2(a)

8.2 The information must be displayed:

a. in the form the PSR specifies

b. prominently on the directed PSP's personal banking homepage for at least 12 months following publication

c. no more than one click away from the most recent information published under this section until at least five years following publication

d. in accordance with any other requirements of a kind mentioned in paragraph 3.4(c)

8.3 For the purposes of paragraph 8.2, 'prominently' means in such a way that the information will come to the attention of a consumer seeking that information (for example, to decide whether to open a current account with a directed PSP).

9 Assurance of information

9.1 A directed PSP must ensure that information it provides to the PSR under section 6 is accompanied by a letter, signed by the chief financial officer of the directed PSP (or a person in an equivalent or more senior position), confirming that it has prepared the information in accordance with:

a. this direction

b. any requirements the PSR makes known to the directed PSP in writing or includes in guidance issued by the PSR

10 Correction of published information

10.1 If a directed PSP finds an error in any information it publishes under this direction that may make the published information materially misleading, it must notify the PSR of the error immediately and:

a. explain the error

b. propose a way to correct the error

10.2 If the PSR informs a directed PSP that it must correct any information published under this direction, the directed PSP must within ten working days correct that information in the manner the PSR specifies.

11 Monitoring

11.1 The PSR may, in writing, require a directed PSP to provide it with information (including clarification) about how the PSP is complying, or proposes to comply, with:

a. this direction

b. any requirements the PSR makes known in writing to the directed PSP or includes in guidance issued by the PSR

11.2 The PSP must provide the information by the date given by the PSR.

12 Application

12.1 This direction applies to the directed PSPs.

13 Commencement and duration

13.1 This specific direction comes into force on [DATE].

13.2 This specific direction continues in force until it is varied or revoked by the PSR.

14 Citation

14.1 This specific direction may be cited as Specific Direction [XX] (Publication of APP scams information).

15 Interpretation

15.1 The headings and titles used in this specific direction are for convenience and have no legal effect.

15.2 The Interpretation Act 1978 applies to this specific direction as if it were an Act of Parliament, except where words and expressions are expressly defined.

15.3 References to any statute or statutory provisions must be construed as references to that statute or statutory provision as amended, re-enacted or modified, whether by statute or otherwise.

15.4 In this specific direction, the word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word and the word 'include' and its derivatives shall be construed accordingly.

15.5 In this specific direction:

- **Act** means the Financial Services (Banking Reform) Act 2013.
- **APP Scam Case** has the meaning given by paragraph 4.1a (key definitions).
- **APP Scam Payment** has the meaning given by paragraph 4.1b (key definitions).
- **APP Scam Receipt Total** has the meaning given by paragraph 6.2c (provision of information to PSR to be prepared for publication).
- **Consumer** means:
    - an individual who, when participating in a payment transaction to which this direction applies, acts for purposes other than a trade, business or profession
    - an enterprise which, at the time of participating in a payment transaction to which this direction applies, is a micro-enterprise as defined in Article 1 and Article 2(1) and (3) of the Annex to Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, or

- a body which, at the time of participating in a payment transaction to which this direction applies, has an annual income of less than £1 million and is:
  - in England and Wales, a charity as defined by section 1(1) of the Charities Act 2011 (meaning of 'charity')
  - in Scotland, a charity as defined by section 106 of the Charities and Trustee Investment (Scotland) Act 2005 (general interpretation)
  - in Northern Ireland, a charity as defined by section 1(1) of the Charities Act (Northern Ireland) 2008 (meaning of 'charity')

- **Consumer Payment** means a payment made by a consumer.
- **Consumer Payment Total** has the meaning given by paragraph 6.2e (provision of information to PSR to be prepared for publication).
- **Faster Payments** means the Faster Payments Scheme.
- **Identified Receiving PSP** has the meaning given by paragraph 6.2b (provision of information to PSR to be prepared for publication).
- **PSP** means a payment service provider within the meaning of section 42 of the Act.
- **Payment System** has the meaning given by section 41 of the Act.
- **Payment Systems Regulator** or **PSR** means the body corporate established under Part 5 of the Act.
- **PSR Reporting Day** has the meaning given by paragraph 4.2b (key definitions).
- **Publication Month** has the meaning given by paragraph 4.2a (key definitions).
- **Reporting Period** has the meaning given by paragraph 4.2c (key definitions).
- **Sending PSP** means, in relation to a payment transaction (including an APP scam payment), the PSP that executes a payment order to transfer funds to the intended recipient in that transaction.
- **Specified Receiving PSP** has the meaning given by paragraph 7.2 (verification of receiving PSP information).
- **Working day** means any day which is not a Saturday, a Sunday, Christmas Day, Good Friday or a day which is a bank holiday in England and Wales under the Banking and Financial Dealings Act 1971.

Made on [DATE]

Chris Hemsley
Managing Director
Payment Systems Regulator

PUB REF: CP21/10

12 Endeavour Square
London E20 1JN
Telephone: 0300 456 3677
Website: www.psr.org.uk