Which?, 2 Marylebone Road, London, NW1 4DF
Date: 15 November 2018
Response to: APP Scams Steering Group Draft contingent reimbursement model code

Consultation Response

Authorised Push Payment Scams Steering Group consultation: Draft contingent reimbursement model code

Summary

- Which? broadly agrees with the Authorised Push Payment (APP) Scams Steering Group's draft contingent reimbursement model code. The draft code is a step towards a system that is fairer to victims of APP scams and it will provide some incentives for those best placed to reduce APP scams to do so, two key aims of Which?'s 2016 super-complaint[1] on this issue.

- We strongly support the principle that all victims meeting their requisite level of care should be reimbursed, regardless of the actions of the sending and receiving payment service providers.[2] We also agree with the requirements on both sending and receiving firms to identify and mitigate the risk of scams, and for sending firms to administer any reimbursement to the victim. However, the code should set out that any report of an APP scam should be treated as a complaint by both the sending and receiving firms.

- The steering group now needs to urgently agree how to fund the reimbursement of victims in 'no blame' cases, where the victim has met the required standard and both the sending and receiving firms have met their obligations under the code, and who will govern the code once it is in force. Choosing the right governance body is fundamentally important for ensuring that all firms involved in push payments sign up to the voluntary code and adhere to it, and for ensuring that the code, and any associated rules, keep pace with how scams evolve.

- Victims in no blame cases should be reimbursed from a central fund that is collectively funded by a transaction charge on sending firms using Faster Payments. Of the seven options proposed by the steering group, a transaction charge, if levied on firms rather than consumers, is one of only two options that could incentivise firms involved in push payments to individually and collectively reduce the risk of APP scams, above and beyond the minimum requirements set out in the code. We are concerned that the other option, a wider contribution mechanism covering firms beyond payment service providers, will be difficult to define and agree in time for the launch of the code in early 2019.

[1] Which? (2016), *Which? super-complaint: Consumer safeguards in the market for push payments*

[2] We use the terms 'sending firms' and 'receiving firms' throughout the rest of this submission in place of 'sending payment service providers' and 'receiving payment service providers'

- We propose that the transaction charge should be paid by the sending firm to the Faster Payments scheme, since it is the sending firm that chooses to use Faster Payments, and its customers benefit from any protections against scams offered by Faster Payments. The Faster Payments scheme should then use this funding to offer a new protection guarantee for customers similar to the Direct Debit Guarantee.

- If a funding mechanism for no blame cases is not ready in time for the launch of the code in early 2019, then the sending firm involved in each case should reimburse the victim.

- The contingent reimbursement model code should be governed by Pay.UK. Unlike other payment schemes, Pay.UK's Faster Payments scheme lacks rules or policies related to consumer protection against fraud. Pay.UK should perform a number of functions, including translating the key principles and requirements of the code into its scheme rules for Faster Payments, which all firms that use the scheme must follow.

Which? broadly agrees with the draft contingent reimbursement model code

Which? welcomes the opportunity to respond to the APP Scams Steering Group's consultation on the draft contingent reimbursement model code. We welcome the work that the Payment Systems Regulator and industry have done since our super-complaint in September 2016 to improve the detection, prevention, and response to APP scams. The contingent reimbursement model draft code is another step towards a fairer and more effective system.

One of the consumer representatives on the steering group is a Which? employee. Here we set out Which?'s views on the draft code.

The current system leaves victims facing losses of potentially life-changing amounts of money to fraudsters whose methods are constantly evolving. Whether a victim is reimbursed after a scam is dependent on the goodwill of their bank, or the success of attempts at repatriation, so most victims are not reimbursed unless the sending and/or receiving firm decides it is at fault. Of the £92.9m lost by consumers from 31,510 cases of APP fraud in the first half of 2018, just £15.4m (16.6%) was returned to consumers.[3]

Which? strongly agrees with the two main aims of the draft code: to reduce the occurrence of APP scams, and to reduce the impact of these crimes. These two aims were at the heart of Which?'s 2016 super-complaint on this issue. The code should be judged principally by how well it achieves both of these aims.

Consumers have important roles to play in preventing APP scams. We support the principles in the code that consumers meeting a requisite level of care should be reimbursed, regardless of the actions of the sending and receiving firms, and that consumers who are vulnerable to APP

[3] UK Finance (2018), *2018 half year fraud update*, p.19

scams should not be held to the same level of care as other consumers. We also support the code's approach to the requisite level of care for consumers, including the requirements for consumers to be open and honest in their dealings with firms.

Which? agrees with the principle that the code should provide incentives for those with the ability to prevent APP scams to do so. Consumers already have extremely strong incentives to avoid being scammed, as they stand to lose significant, sometimes life-changing sums of money, as well as potentially experiencing distress, fear and embarrassment. However the firms involved in making push payments currently lack the financial incentives to reduce APP scams.

This is unlike other payment methods, whereby firms have arrangements for appropriately allocating between themselves the liability for losses due to fraud. Sending and receiving firms, and the operators of the payment schemes, therefore have strong financial incentives to develop effective systems and approaches for reducing the risk of other types of fraud, and have introduced a range of protections and policies.

The code therefore rightly sets out a range of requirements on both the sending and receiving firms. If either firm does not meet these standards, and the consumer has met their requisite level of care, then the firm/s will be required to reimburse the victim. This will therefore provide financial incentives on firms to meet these industry standards. Crucially the code makes clear that both the sending and receiving firms have a responsibility to identify and mitigate the risks of scams, above and beyond administering the payment. We particularly support the requirements on sending firms to:

- provide effective warnings to their customers, which should be understandable, clear, impactful, timely and specific;
- intervene on a risk-based approach to delay execution of a payment authorisation; and
- provide a greater level of protection for customers who are considered vulnerable to APP fraud.

Equally, the code makes clear that receiving firms have a responsibility to mitigate the risks of APP scams, since fraudsters directly, or indirectly, use accounts with them. We therefore strongly support the requirements on receiving firms, including to:

- screen customer accounts to identify accounts at higher risk of being used by criminals;
- use transactional data and customer behaviour analytics to identify payments that are at higher risk of being an APP fraud; and
- train their employees on how to identify indicators of circumstances around, and leading to, transactions that are at higher risk of facilitating APP fraud.

We also support requirements for both the sending and receiving firms to introduce Confirmation of Payee. This measure is urgently required to tackle APP scams, and it is disappointing that voluntary action to introduce Confirmation of Payee has not resulted in swifter implementation. Payments made via Faster Payments are currently processed without checking whether the account name matches the account number. Confirmation of Payee will verify the name of the company or individual connected to that account before any money is transferred. If this provides consumers with clear and reliable information and warnings, this measure could be particularly effective at tackling redirection scams, where the victim thinks they are paying a legitimate payee but are tricked into paying a malicious payee. Consumers lost £43.7m to these scams in the first half of 2018.[4]

While we support the key principles and requirements in the code, whether the code meets its stated aims will depend on how the code is put into practice by signatories to the code, and how they are held to account. Crucially, the code should not place unrealistic expectations on victims. Firms should be required to show clear evidence that their warnings are effective, both that their systems are designed to be effective for different groups of consumers and that these warnings were effective in individual cases. If they are unable to evidence this, then consumers who have met their requisite level of care should be reimbursed.

The code needs to be updated to keep pace with fraudsters' rapidly evolving methods. There is a risk that many firms will be able to meet the proposed minimum standards, particularly those that relate to their general systems and processes, but that the number and value of APP scams will continue to rise. A strong governance body is required that has the ability to introduce new measures to combat scams that are adopted across the sector. Furthermore, the steering group needs to agree a funding mechanism for no blame cases that provides a financial incentive on firms to work individually and collectively to go above and beyond the code. We set out our proposals below on why Pay.UK, the operator of Faster Payments, should be the governance body, and for Pay.UK to introduce a transaction charge on its member firms to fund no blame cases.

The code should also lead to a system that is not onerous for consumers to report APP fraud and pursue their claim for reimbursement. Consumers should not be expected to understand each firm's role in the push payment, and how this relates to industry standards. Nor should they have to deal with the receiving firm, since they are not a customer of that firm. We therefore support the code's requirement for the sending firm to administer any reimbursement, and to make this reimbursement swiftly, even if the sending and receiving firms have yet to agree on how to apportion these costs.

However, the code currently states that where a customer reports that they have been a victim of an APP scam, this report may not meet the definition of a complaint. This is not in line with the FCA's definition of a complaint as 'any oral or written expression of dissatisfaction, whether justified or not… which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience'.[5] When a consumer reports an APP fraud, both the sending and receiving firms should automatically count this as a complaint since it is not reasonable to expect consumers to know which firm might potentially have failed to meet their obligations. This would ensure that the FCA's time periods for resolving complaints are always

[4] UK Finance (2018), *2018 half year fraud update: Annexe*
[5] The full definition is: 'Any oral or written expression of dissatisfaction, whether justified or not, from, or on behalf of, a person about the provision of, or failure to provide, a financial service or a redress determination, which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience.'
https://www.handbook.fca.org.uk/handbook/glossary/G197.html

triggered as soon as a consumer reports an APP fraud, and that consumers are not required to wait for an initial response to then have to submit a complaint, before then potentially taking their complaint to the Financial Ombudsman Service.[6]

The steering group urgently needs to agree how to fund the reimbursement of victims in no blame cases, and who will govern the code

The steering group has not been able to agree so far on how to fund the reimbursement of victims in no blame cases, where both the victim and the firms involved have met their obligations under the code, and on who will govern the code. Both issues are fundamentally important for the success of the scheme and need to be urgently addressed in time for the launch of the scheme in early 2019.

Without a funding solution for no blame cases, many victims that have met the code's requisite level of care may not be reimbursed, despite this being a key principle of the code. As well as failing to address the detriment experienced by these victims, this could severely undermine public trust in the scheme.

As well as finding a solution to reimburse victims, the funding mechanism for no blame cases should be designed to provide continuing financial incentives for sending and receiving firms to go above and beyond the code's industry standards to adapt to fraudsters' changing methods. This can be challenging given that:

- firms are reliant on the actions of other firms to reduce the likelihood of their customers being scammed as the fraudster may bank with someone else; and
- the majority of the benefit from a firm guarding against its customers being fraudsters is likely to go to customers of other banks, who would otherwise have lost money to fraud.

This means that industry measures to combat scams often require collective action, which can be difficult to achieve. Such industry-wide measures will only be adopted if there are strong incentives on all firms and the relevant payment scheme to bear down on APP scams.

For example, plans by Pay.UK and members of Faster Payments to introduce Confirmation of Payee would arguably have been introduced sooner had there been stronger incentives on Faster Payments and its member firms to reduce scams since Faster Payments launched in 2008. Confirmation of Payee was considered at least as early as 2011 by the then Payments Council,[7] and later in 2015 by Payments UK, which is now part of UK Finance.[8] But progress has been slow, especially as it became unclear whether all firms would offer the service, and when those that chose to offer it would make it available. The Payment Systems Regulator has been

[6] Separately, Which? has welcomed the Financial Conduct Authority's (FCA) proposals to require receiving firms to follow the FCA's complaints handling rules, and to enable consumers to appeal to the Financial Ombudsman Service (FOS) if they are not happy with how their complaint is handled. See Which? (2018), *Response to FCA consultation on 'Authorised push payment fraud – extending the jurisdiction of the Financial Ombudsman Service'*
[7] Payments Council (2011), *National Payments Plan*
[8] Payments UK (2015), *World Class Payments in the UK*

forced to step in. It recently announced plans to consult on using its regulatory powers to give a 'general direction' to banks and payment service providers to implement Confirmation of Payee.[9] Which? strongly supports the Payment Systems Regulator's proposals.

Choosing the right governance body is also fundamentally important for the success of the code. The governance body should be accountable for achieving the aims of the code. It should therefore have strong incentives to encourage new industry-wide protections against scams that go above and beyond the existing code. But unless it is in a position to lead the development and implementation of these measures, it will be difficult for any progress to be made. Choosing the right governance body can also help to:

- encourage all firms involved in push payments to sign up to the voluntary code;
- evidence that firms are adhering to the code, both in their systems and in individual cases;
- resolve disputes between firms regarding reimbursement decisions; and
- continuously update the code, and any associated rules, to keep pace with how APP scams evolve.

The steering group has also not been able to decide what should happen when the victim and either or both firms have not met their obligations under the code. So a sending or receiving firm, or both, could fail to meet the standards in the code but face no penalty for doing so. For the code to be effective there should be strong financial incentives on firms to meet the code's standards, regardless of the actions of victims.

Victims in no blame cases should be reimbursed from a central fund collectively funded by a transaction charge on sending firms

If firms involved in push payments were to collectively fund no blame scenarios, this would provide incentives for sending and receiving firms to work individually and collectively to reduce the risk of APP scams, including by putting pressure on Pay.UK to require all of its members to introduce new protections against scams, such as Confirmation of Payee. In turn, this would reduce the cost to firms.

Only two of the steering group's proposals could potentially require firms involved in push payments to collectively fund no blame scenarios:

- creating a contribution mechanism across all parties with an ability to prevent APP scams from occurring (for example, firms, telecoms companies, data handlers etc); and
- a transaction charge on higher risk and higher value payments to be directed into a fund.

Some stakeholders have proposed that the transaction charge option above could be paid directly by consumers. However, this would not provide any incentive on firms involved in push

[9] The Payment Systems Regulator has proposed deadlines of 1 April 2019 for responding to Confirmation of Payee requests and 1 July 2019 for sending Confirmation of Payee requests and presenting results to their customers. https://www.psr.org.uk/psr-publications/news-announcements/PSR-welcomes-industry-code-to-protect-against-app-scams

payments or Faster Payments to reduce APP scams. It could also act as a barrier to consumers making transactions or lead them to use other less well-suited or riskier payment methods (e.g cash for large transactions). The transaction charge should therefore be levied on firms rather than consumers.

Similarly, most of the steering group's other proposed funding options would provide no incentives on firms involved in push payments to collectively reduce APP scams. Some, such as unlocking dormant funds, involve funding sources with no link to where the risks of APP scams can be mitigated. Some of these proposed options, such as consumers taking out insurance products, would also add barriers to consumers when making payments.

Of the two options above, we are concerned that the contribution mechanism across all parties will be difficult to define and agree in time for the launch of the code in early 2019. In contrast, Pay.UK already collects funding from members of Faster Payments, so a transaction charge levied just on its members firms could form part of this funding. The APP Scams Steering Group also has representatives from banks, the Electronic Money Association and UK Finance, whereas firms from other sectors are not currently represented.

We propose that the transaction charge should be paid by the sending firm to the Faster Payments scheme. This is because it is the sending firm that chooses the payment options for its customers. Its customers then benefit from any protections offered by those payment methods. It therefore has strong incentives to push for greater protections for its customers. The sending firm can also choose to offer its customers alternative methods of push payments, such as Visa Direct and Mastercard Send which launched recently, or to recommend that customers use other payment methods, such as card payments or PayPal.

We propose that this levy should form part of a new Faster Payments guarantee for consumers, similar to the Direct Debit Guarantee and card payment chargeback rules. The Faster Payments guarantee would make clear to consumers that they will always be reimbursed if they have met their requisite level of care when making a payment via Faster Payments.

Furthermore, we propose that Pay.UK should also levy an additional charge on firms that do not meet the standards of the code in cases where the victim has not met their requisite level of care. This would ensure that firms always have strong financial incentives to meet the code's standards. We do not think that these charges are likely to be sufficient to fund no blame cases, so this funding would be in addition to our proposed transaction charge on sending firms.

However, if our proposed funding mechanism for no blame cases is not ready in time for the launch of the code in early 2019, then the sending firm in each case should reimburse the victim until the funding mechanism launches. This is the simplest and most practical option to ensure that the code delivers on the principles agreed by the steering group until a longer term funding mechanism is agreed and implemented for no blame cases.

The contingent reimbursement model code should be governed by Pay.UK

At the heart of all APP scams is the relevant payment system. The draft code applies to three payment systems:

- the Faster Payments scheme, which is operated by Pay.UK;
- the CHAPS payment system, which is operated by the Bank of England; and
- internal book transfers, which involve payments made to and from the customer of the same payment service provider.

The code does not currently place any requirements on the operators of these schemes, Pay.UK and the Bank of England. This is despite the Payment Systems Regulator concluding in response to our super-complaint that neither the Faster Payments scheme nor the CHAPs scheme have any rules, policies or procedures related to consumer protection against scams.[10]

Other payment schemes have rules that protect consumers against fraudulent payments, including mechanisms for payments to be challenged and reversed. For example:

- Card schemes provide the interbank challenge and reversal process referred to as chargeback. The chargeback rules are highly detailed, and are updated on a frequent basis to take into account constantly changing fraud and behaviour patterns. For example, Mastercard's current Chargeback Guide is more than 400 pages.[11]
- Direct debits, which are operated by Pay.UK, are covered by the Direct Debit Guarantee. The paying firm is responsible for making any refunds immediately if an error is made in the payment of a direct debit. If the recipient has made the error then the sending firm must raise an indemnity claim to obtain the money back. If the recipient no longer exists, the receiving firm will settle the indemnity claim.

Chargeback and similar arrangements provide not only a means of reimbursing consumers, but also of shifting costs onto the receiving bank if they are at fault (or the merchant acquirer in a card scheme). So these interbank processes provide for liability to be passed to the receiving firm where the fraudster holds or operates an account. Liability is therefore allocated to those who are best able to manage the risk of fraudsters using bank accounts and payment systems to facilitate their scam.

Both the Faster Payments and CHAPs schemes should incorporate the principles of the code into their detailed scheme rules. Pay.UK should lead the governance of the contingent reimbursement model code due to the prevalence of APP scams on its system. Our analysis of UK Finance figures shows that in the first half of 2018, 96.2% (47,520) of APP payments where scams were reported, excluding international payments which are not covered by the code,

---

[10] The Payment Systems Regulator concluded: 'The operators of the Faster Payments Scheme (FPS) and CHAPS payment systems, the two payment systems which consumers might use when falling foul of APP scams, do not have any rules, policies or procedures in place related to consumer protection against fraud or scams. Operators of these systems view it as outside their remit to intervene in what they view as private contractual matters between PSPs and their customers.' Payment Systems Regulator (2016), *Which? authorised push payments super-complaint: PSR response*, p.5

[11] Mastercard (2018), *Chargeback Guide*

were made via Faster Payments. Just 0.7% (355) were payments made via CHAPs and 1.9% (921) via internal bank transfers.[12] All members of Faster Payments are required to follow its scheme rules, so this would ensure that the code is adopted across the industry. Pay.UK is also independent of its members firms, as required by the Bank of England's governance code of practice.

Pay.UK should:

- translate the key principles and requirements of the code into its scheme rules for Faster Payments, which all firms that use the scheme must follow;
- audit member firms' systems to evidence whether these meet the standards in the code, including whether warnings provided to consumers are effective;
- levy our proposed transaction charge on firms making payments via Faster Payments, which should be used to fund a new protection guarantee for consumers that meet their requisite level of care when making a payment, as well as to fund the governance and implementation of the code, such as new central systems or infrastructure;
- introduce a dispute mechanism for disputes between members of Faster Payments regarding APP scams;
- ensure that its wider governance structure, and any specific governance for the code, is independent of its member firms, and has strong consumer representation; and
- report regularly on the effectiveness of the code, and consult on changes to update the code and any associated rules.

About Which?

Which? is the largest consumer organisation in the UK with more than 1.3 million members and supporters. We operate as an independent, a-political, social enterprise working for all consumers. We are funded solely by our commercial ventures and receive no government money, public donations, or other fundraising income. Which?'s mission is to make individuals as powerful as the organisations they have to deal with in their daily lives, by empowering them to make informed decisions and by campaigning to make people's lives fairer, simpler and safer.

For more information, contact Alastair Reed, senior policy adviser
alastair.reed@which.co.uk

November 2018

[12] Note, UK Finance also reports figures for BACS payments (568) and standing orders (29). UK Finance (2018), *2018 half year fraud update: Annexe*