September 2018

APP Scams Steering Group

Draft Contingent Reimbursement Model Code

CONSULTATION PAPER

The Authorised Push Payments Scams Steering Group (Steering Group) was established by the Payment Systems Regulator in March 2018 to lead the development of a voluntary industry code for the reimbursement of victims of authorised push payment scams.

The Steering Group now offers up for consultation a draft Code. Comment, discussion and representations from any respondents are encouraged in respect of any of the elements of the draft Code and responses should clearly identify what they wish to see altered and the reason why the alteration should be made. Respondents are welcome to provide alternative suggestions. As a result, the terms of the draft Code may well change.

During the consultation period, Payment Service Providers (PSPs) may consider whether or not to adopt elements of the draft Code. That is an entirely voluntary matter. In view of the broad range of PSPs across the payments industry, it will be for each PSP to determine which elements of the draft Code it applies to the transfer of funds during the consultation period.

The Steering Group's objective was to lead on the development of a voluntary industry code. This has led to a continued evolution in thinking, understanding and interpretation of complex issues. PSPs should each take their own legal and other advice in connection with the draft Code and this consultation document, and any actions they may or may not take during the consultation period.

The draft Code and this consultation document do not contain any legal advice to any person or PSP, and is no substitute for formal legal advice required by any person or PSP. The Steering Group does not accept any legal responsibility or liability for the actions or omissions of any person or PSP in relation to or reliance on the draft Code or this consultation document.

CONTENTS

1. SUMMARY

1.1. Authorised push payment (APP) scams – where people are tricked into sending money to a fraudster – are crimes that can have devastating effects on victims. According to statistics published by UK Finance, consumer losses on APP scams in the first half of 2018 totalled £92.9 million across 31,510 cases. The amount of money returned to consumers was £15.4 million (or 16.5% of the total value), which is made up of partial or total recovery of the funds as well as goodwill payments made by firms in some cases.

1.2. In September 2016, the consumer body Which? submitted a super-complaint to the Payment Systems Regulator (PSR) about APP scams, raising its concerns that victims do not have enough protection. The PSR investigated the issue and the concerns raised, and in December 2016 found that more needed to be done to tackle APP scams. The PSR and industry undertook further work, and in November 2017, the PSR published the findings and outcome of this work. This included a consultation on the introduction of a Contingent Reimbursement Model (CRM). The model sets out the circumstances in which payment service providers (firms) would be responsible for reimbursing APP scam victims who have acted appropriately. In February 2018, after taking the consultation responses into account, the PSR considered a CRM – formalised into a voluntary industry code of good practice – is an effective way to reduce the occurrence of APP scams and the devastating harm they cause consumers.

1.3. In March 2018, a steering group was established, made up of an equal balance of industry (payment service providers) and consumer representatives, to develop a proposal for a CRM and formalise it into a voluntary industry code. Key regulatory and government bodies are observers on the group.

1.4. The steering group was expected to Issue a draft code for public consultation by the end of September 2018. The code is intended to be finalised in early 2019

1.5. The main aim of the code is to reduce the occurrence of APP scams from happening in the first place, and lessen the impact these crimes have on consumers, microenterprises and small charities (referred to as customers – see paragraph 3.24). The steering group considers that the draft code should achieve this. It incorporates existing good industry practice for preventing APP scams and helping these customers protect themselves from these crimes, while ensuring customers remain vigilant. Facing a challenging timeframe, there are some outstanding areas of work to resolve (which we outline below) and we are committed to working hard to do this by early 2019.

1.6. This consultation document sets out the rationale and intent of the various provisions in the draft code. It also sets out those issues on which the steering group has not yet reached consensus and will be undertaking further work during the consultation period to resolve. The steering group is now seeking views on the draft code and these areas of further work so that these can be considered.

Reimbursement under the draft code

1.7. The steering group have agreed proposals for a set of reimbursement principles depending on whether the relevant parties had met their expected levels of care. This is summarised at a high level in figure 1.

		Customer	
		Level of care met	Level of care not met
Firms	Levels of care met	Customer reimbursed (see para 1.9 on the funding issue)	Customer not reimbursed
	Levels of care not met	Customer reimbursed	Still under discussion
Customers that are considered vulnerable to APP scams receive additional protection and a different reimbursement approach (see para 3.65 onwards)			

Fig. 1 – Reimbursement outcomes

1.8. The steering group agrees that a customer that has met their requisite level of care should be reimbursed. There may be instances where a victim of an APP scam has met their requisite level of care, and so should be reimbursed, but no firm involved in the payment journey has breached their own level of care.

1.9. The steering group has not been able, so far, to resolve the question of who should meet the cost of reimbursements in these circumstances. The steering group will continue to work hard during the consultation period to consider and identify a sustainable funding mechanism through which to reimburse customers in such a scenario.

1.10. In addition, the steering group will continue work to consider:

- what should happen when both firms and customers have not met their levels of care,
- the evidential approach that will underpin the code,
- a mechanism for inter-firm allocation of reimbursement costs and dispute resolution between firms, and
- the governance of the code once it is finalised.

Status of the draft code

1.11. Until the funding solution and other outstanding issues are agreed and a final code is published, the draft code is not 'in force'.

1.12. From today, however, retail banks represented on the steering group have individually committed to work towards implementing the standards for firms and, in principle, the customer requisite level of care set out in the draft code. The steering group recognises that some standards may take firms some time to implement. The steering group urges other firms that provide payment services to follow this example.

1.13. In the period between now and the publication of a final code, until a funding solution is identified for the scenario where all parties have met their expected levels of care, customers in this scenario will not be reimbursed (unless firms decide to make a goodwill payment). The steering group intends

to revisit whether these victims could be reimbursed once the funding mechanism has been agreed. Once a final code is issued, retail banks represented on the steering group have individually committed to implementing the final code in full in early 2019. The steering group hopes that all firms will follow this example, though it is acknowledged that the timeframes for firms to implement all elements of the code will vary. Firms are urged to do what they can to raise standards and improve customer protections between now and the publication of the final code, and after that to implement the full code as quickly as practicable.

Next Steps

1.14. The steering group is now consulting stakeholders to assist in further developing the code.

1.15. The steering group invites feedback before 5pm on Thursday 15 November 2018. We have set out a non-exhaustive list of consultation questions in Section 5.

1.16. **Publication of consultation responses:** please mark any information contained in your response which you consider should not be published on the steering group website because it is confidential or commercially sensitive information clearly. Please also provide a non-confidential version which can be published on the website.

1.17. **Providing confidential information:** please note that if there is any information in your response that you do not wish all members of the steering group[1] to see, please mark this clearly. In such a case, only the group's Chair and the group's independent adviser will see the information. They will be assisted in preparing the anonymised information and ensuring it is reflected appropriately by a fully independent economic consultancy. The Chair, independent adviser and consultancy will provide the information to the rest of the steering group on an appropriately anonymised basis. Please also provide a non-confidential version which all members of the group can see.

1.18. At the request of the steering group, the PSR will, for administrative reasons, collect responses and pass these on to the steering group's Chair and the independent adviser.

Please send your responses to app-scam-pso-project@psr.org.uk

or in writing to:

APP scams Steering Group Consultation
c/o Payment Systems Regulator
12 Endeavour Square, Stratford
London E20 1JN

[1] See para 2.8 for details of members

2. BACKGROUND

2.1. Authorised push payment (APP) scams are where people are tricked into sending money to a fraudster. They are crimes that can have devastating effects on victims. According to statistics published by UK Finance, consumer losses on APP scams in the first half of 2018 totalled £92.9 million across 31,510 cases. The amount of money returned to consumers was £15.4 million (or 16.5% of the total value), which is made up of partial or total recovery of the funds as well as goodwill payments made by firms in some cases. It is the second biggest type of payment fraud reported by UK Finance, in terms of both the number of scams, and the total value involved (behind card fraud). We set out some different types of APP scams in the Annex to this consultation paper.

2.2. In September 2016, the consumer body Which? submitted a super-complaint to the Payment Systems Regulator (PSR) about APP scams, raising its concerns that victims don't have enough protection. The PSR investigated the issue and the concerns raised, and in December 2016 published its response. Following this, in November 2017, the PSR found that more needed to be done to help prevent APP scams, and reduce the impact these crimes have on victims.[2] It consulted on the introduction of a CRM, which would set out the circumstances for when payment service providers (firms) would be responsible for reimbursing APP scam victims who have acted appropriately. The CRM would set out good practice measures and processes that firms should follow which should help reduce the occurrence of APP scams, and the expectations on consumers to help protect themselves.

2.3. In early 2018, taking account of responses, the PSR considered that an industry code of good practice, developed collaboratively by industry and consumer group representatives, that sets out the CRM's rules is the most effective way to promote the interests of users of payment system services and reduce the consumer harm that APP scams can cause.[3]

The APP scams Steering Group

2.4. A dedicated steering group was established in March 2018 by the PSR, tasked with developing the CRM and formalising it into a voluntary industry code of good practice.

2.5. The steering group has an independent chair, Ruth Evans. There are twelve members – consisting of an equal balance of industry and consumer representatives.

2.6. The steering group has been responsible for reaching consensus between members on key issues, and formalising the CRM into a proposed voluntary industry good practice code for reimbursement of APP scam victims.

2.7. The PSR is supporting the group and driving the timeframe. Other key regulatory and governmental bodies have been involved as observers – including the FCA, HM Treasury, the Home Office, the Financial Ombudsman Service (FOS), City of London Police and the National Trading Standards. UK Finance has provided secretariat support to the Group.

2.8. A full list of members can be seen on our website, www.appcrmsteeringgroup.uk, along with summaries of each steering group meeting, and our Terms of Reference[4].

[2] https://www.psr.org.uk/sites/default/files/media/PDF/PSR-APP-Scams-report-consultation_1.pdf

[3] https://www.psr.org.uk/sites/default/files/media/PDF/Outcome_of_CRM_Consultation_Feb_2018.pdf

[4] https://appcrmsteeringgroup.uk/wp-content/uploads/2018/04/ToR-for-Endorsement-at-27-April-meeting.pdf

Core Principles

2.9. The steering group established a set of core principles for the code that we expect our proposals to be consistent with. These are principles that we consider underpin an effective CRM that should better protect customers from harm. Amongst others, these include principles to provide the right incentives for those parties who can best reduce the occurrence of APP scams and respond to them, to deliver consistent outcomes for parties with the same circumstances, and to be based on measures that are likely to be effective at preventing and responding to APP scams.

2.10. The core principles and operating principles, as set out in the Terms of Reference, are shown in the boxes below.

Core Principles

i. Incentives for those with the ability to effectively prevent APP scams and reduce their impact: *The code must be designed so that those parties with the ability to effectively influence APP scam prevention and response at different stages of the payment journey are incentivised to do so. Ultimately, the incentives generated by the code should reduce the number of APP scams that would otherwise occur.*

ii. Consistency of outcomes: *The code should deliver consistent outcomes for parties8 with the same circumstances. For example, an inconsistent outcome would be where there were two victims of separate scams that shared the same characteristics, one was reimbursed and one was not. Consistency of outcomes does not mean that reimbursement for each of the victims should necessarily come from the same source of funds.*

iii. Leverage existing and future initiatives that are likely to be effective at preventing and helping respond to APP scams: *There are a range of measures highlighted by the PSR that are aimed at assisting APP scam prevention and response, which have been recently deployed or are currently under development. This includes the Best Practice Standards, Confirmation of Payee, and transaction data analytics. The code must leverage these and future measures, and incentivise their use and development by including them in the standards of care that PSPs should meet.*

iv. Adoption by all PSPs that have an element of control over preventing and responding to APP scams: *PSPs that have an element of control over payments within scope of the code, must adhere to it.*

v. No contingency on the recovery of funds: *The implementation of the code must not be contingent on the recovery of funds in specific cases.*

vi. No adverse impact on PSP ability to make goodwill payments: *The code must not displace or constrain the ability of PSPs to make goodwill payments to victims of APP scams in situations they deem it appropriate to do so.*

vii. No adverse impact on commercial development of further protections: *The code must set out the minimum level of care that PSPs must take to protect consumers from harm caused by APP scams. It must not restrict the ability of individual PSPs, or other parties, to develop and offer products to consumers that provide additional protection.*

viii. Capability for becoming part of the relevant considerations that the FOS takes into account: *The code must be developed in such a way that it is capable of becoming part of the relevant considerations that FOS can take into account when determining outcomes of a consumer complaint about APP scams.*

Operating Principles

- Simplicity: *The rules adopted should be as simple as possible to be effective, for both PSPs and potential code beneficiaries. The experience for victims seeking reimbursement should be simple and easy to understand.*
- Transparency: *The code should be developed, implemented and operated in an open and transparent manner (to the extent that privacy and security considerations permit).*
- Timeliness: *The rules adopted should support timely reimbursement and expedited communication between PSPs and consumers.*
- Fairness: *The code should be developed, implemented and operated in a fair and publicly defensible manner.*
- Costs, benefits and impact: *The rules and standards in the code should be justifiable – both individually and as a whole – on the basis of their costs and benefits, in particular their impact on the harm caused by APP scams.*

3. THE DRAFT CODE

3.1. The draft code is presented for consultation. When 'code' is referred to in this section, it means the draft code. The code is a voluntary code. It sets out good industry practice for preventing and responding to APP scams, and the requisite level of care expected of customers to protect themselves from APP scams.

3.2. The code is designed to be adopted for the benefit of both firms and customers, with the overall aim of reducing the occurrence of APP scams and the harm caused to victims.

3.3. Firms that adopt the code should follow the Standards for Firms, as well as the more general good practice set out in the Annex to the code, to resolve or prevent customer complaints and avoid the need for these to be referred to the FOS.

3.4. The steering group has designed the code to ensure victims of APP scams are able to get their money back, provided they meet the requisite level of care. This reimbursement would be administered by their firm (the sending firm).

3.5. The steering group has also said that if a firm within the scope of the code fails in some respect to meet the Standards for Firms, then that firm should meet the cost of the reimbursement, in whole or in part (eg where more than one firm did not meet the standards – see paragraph 4.21 onward). As stated in paragraph 1.9, the steering group will continue to work hard during the consultation period to identify a sustainable funding mechanism through which to reimburse customers where all parties have met the required standards. See also paragraph 4.1 below.

3.6. In the rest of the paper, the provisions in the draft code and how it should operate are explained, along with the areas where the steering group has not reached consensus and will be doing more work.

3.7. In overview, the provisions of the draft code set out:

- overarching principles
- general expectations on firms
- standards for firms for detecting, preventing and responding to APP scams
- the circumstances in which customers, including customers vulnerable to APP scams, can expect to be reimbursed
- governance of code

3.8. There is also an Annex to the draft code.

3.9. The steering group welcomes feedback on the draft code and any specific provisions. We have included a non-exhaustive list of Consultation Questions at Section 5.

Overarching Provisions: OP1- OP2

3.10. The code should incentivise the parties involved to take action to prevent and respond to APP scams where they are best placed to do so. Firms should be incentivised to implement and use measures that effectively prevent and assist with the response to APP scams, and customers should be incentivised to remain vigilant. This should help minimise the number of APP scams as more is done to stop them happening in the first place. When APP scams do happen, reimbursing the victims – where they could not have reasonably protected themselves – reduces the customer harm.

3.11. Furthermore, the code should be implemented in a way that minimises unnecessary disruption to legitimate payments.

3.12. In line with the steering group's core principles, OP2 makes it clear that the code should not have an adverse impact on firms making discretionary reimbursement payments to customers.

Definitions and Scope of the draft code: DS – DS2

3.13. The code covers scams perpetrated through authorised push payments made in the UK by consumers, microenterprises and small charities. Specifically, these are payments made over the

Faster Payments Service and CHAPS payment systems and internal book transfers[5]. The code applies only to domestic payments; it does not apply to international payments or payments made in other currencies. This aligns with the scope set out by the PSR in its Outcome on the CRM Consultation.[6]

3.14. The code is 'payment channel neutral'. In other words, it applies regardless of how a customer interacts with their firm to authorise a payment, be it by telephone, online banking, or mobile smartphone apps.

3.15. When an APP scam occurs, the fraudster often moves the money from the first receiving account (the first generation account) on to other accounts. The code only applies to firms involved in authorising and processing the transaction from the victim to the first generation account. These firms should consider whether they met their standards of care and if they should be responsible for reimbursing the victim if eligible.

3.16. The steering group identified some areas where there might be uncertainty whether the code applies or not. At DS2(2) we set out some examples of things that are outside scope.

3.17. The code is aimed solely at APP scams. The essential element of APP scams is that the payment involved must be authorised. The Payment Services Regulations 2017[7] set out the circumstances in which a payment is considered authorised. This has been adopted in the code (set out at DS1(2)(a)). Broadly speaking, a payment will only be authorised when a customer consents to the making of the payment. Where payment is not authorised, it is an unauthorised payment.

3.18. A customer who is the victim of a fraud where the payment was an unauthorised payment would be covered by the separate regime covering unauthorised payments under the Payment Services Regulations[8]. Unauthorised payments are not covered by the code. An example of unauthorised fraud is where a fraudster gains access to a person's bank account without that person realising.

3.19. If a payment made by a customer does not involve being victim to an APP scam, this payment is not covered by this code. Where a customer has some sort of complaint about making such a payment, then it would be covered by their firm's existing complaints process.

3.20. For the code to apply, an APP scam must have taken place. Where a customer has made an authorised payment to another, and, although not having been defrauded, is unsatisfied for some reason as a result, this code will not apply. This is because there will be a legitimate supplier to complain to, for example under the Consumer Rights Act 2015.

3.21. It is proposed, when a final code is published, that it will not be expected to apply to APP scams which took place before publication. However, this should not deter firms who wish to apply it in such instances.

3.22. The steering group has defined important words used in the code for clarity. Many of the definitions are aligned with, or refer to, terms used in the Payment Services Regulations 2017.

3.23. We have used 'Firm' to cover all payment services providers, by adopting the wide, inclusive definition from the Payment Services Regulations 2017. Where we use 'sending firm', this means the firm used by the customer to execute the payment order. Similarly, 'receiving firm' means the firm holding the account used by the fraudster to receive the money.

3.24. Because the code covers consumers, microenterprises and small charities as defined under the Payment Services Regulations 2017, we have used 'Customer' to refer to all of these.

[5] Internal book transfers are where both the sending and receiving payment accounts are held with the same firm, and the transfer would otherwise have been executed across Faster Payments or CHAPS

[6] https://www.psr.org.uk/sites/default/files/media/PDF/Outcome_of_CRM_Consultation_Feb_2018.pdf

[7] Payment Services Regulations 2017 (SI 2017/ 752) at Regulation 67.

[8] Part 7, Payments Services Regulations 2017.

General Expectations of Firms: GF(1) – (3)

3.25. The code includes a section setting out good practice that firms should undertake more generally to help prevent and respond to APP scams. This is in addition to specific good practice set out in the Standards for Firms, discussed below.

3.26. The general expectations on firms would include:

- participation in customer education and awareness campaigns – this will help customers be better informed as to how they can protect themselves from APP scams, so reducing fraud overall;
- Collection of statistics – this will help firms, trade bodies and consumer organisations to understand how APP scam trends are being affected, and so how to improve initiatives to reduce them further;
- Aftercare for customers – this will help reduce fraud overall by providing extra help and tools to prevent people becoming repeat victims.

Standards for Firms: SF, SF1 and SF2

3.27. Firms should be incentivised to implement and use measures that effectively prevent, and assist with the response to, APP scams. This will help reduce the occurrence of APP scams, help customers avoid being becoming victims, and prevent criminals from receiving the proceeds of their activities.

3.28. The Standards for Firms provisions are designed to achieve this by making those firms that do not meet their standards responsible for reimbursing the victim. When assessing whether a firm did not meet its standards, the firm can consider whether compliance with the standard would have helped prevent the APP scam. This is set out in the overarching SF provision.

3.29. The Standards for Firms cover three things – detection, prevention, and response. They differ slightly for firms acting as the 'sending' firm, and those as the 'receiving' firm. By this we mean, a firm's role when it acts for the originating customer authorising the payment (covered by SF1), and when it acts for the payee (covered by SF2). Only the 'first generation' receiving firm falls into the Code (see paragraph 3.15).

Detection

3.30. Here, the draft code encourages firms to better protect customers by building on and improving systems already in place under legal and regulatory requirements to detect potential APP scams. By getting better at analysing transaction data for unusual patterns in payment transactions, detecting payment authorisations, and accounts account holders that present a higher risk of facilitating APP scams, will become easier. The Annex to the code describes some APP scam prevention measures and tools currently available or being implemented.

3.31. Firms should make sure their staff receive training on how best to use the results of these analytics, and how to detect other indicators of risk when speaking or interacting with customers.

Prevention

3.32. These provisions are about helping customers to help protect themselves from falling victim to an APP scam. There are two main strands – Confirmation of Payee, which is discussed further below, and providing effective warnings to customers during payment journeys.

3.33. The steering group wants to incentivise those with the expertise and ability to prevent APP scams effectively, and to reduce its impact. Therefore, the code sets a standard for firms to use their expertise to provide their customers with effective information, at key stages in a payment journey, so that customers have a better chance to protect themselves against being defrauded.

3.34. To do this, at SF(2) there is a proposed framework for firms to provide effective warnings to their customers. As part of this, there are five minimum criteria (at SF1(2)(e)) that effective warnings should meet. They should be:

- Understandable – in plain language, intelligible and meaningful to the Customer;
- Clear - in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's Principles for Businesses;
- Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;
- Timely – given at points in the Payment Journey most likely to have impact on the Customer's decision-making;
- Specific – tailored to the customer type and the APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.

3.35. A constituent element of an effective warning should be that the customer is given clear guidance about action they should take to help avoid the risk that they might be about to fall victim to an APP scam. The customer should also be made fully aware of the consequences if they do not follow those actions and proceed with the payment. That is, that they might not be reimbursed. The warning should also notify the customer whether other payment methods which may be more appropriate to their circumstances are available – for example where a customer is using an online market platform that they might want to pay through that platform.

3.36. The code is payment channel neutral – it would be up to firms to work out how best to provide effective warnings for each channel they provide their customers.

3.37. These effective warnings should build on the education campaigns spoken about in GF(1) above, and on the general information provided by firms to their customers about actions that can be taken to avoid becoming the victim of APP scam.

3.38. Sending firms should also do more for customers identified as vulnerable to APP scams. This will be discussed in more detail below at paragraph 3.65 onward.

Confirmation of Payee

3.39. Confirmation of Payee (CoP) was one of the initiatives proposed by the Payments Strategy Forum, and should have a significant impact on certain types of APP scams.

3.40. The steering group's core principle (iii) is that the code should take advantage of future initiatives that are likely to be effective at preventing and helping respond to APP scams. This includes the use by firms of CoP. The steering group has worked closely with the NPSO to date, and has positioned the code to align with CoP's development. However, until CoP is fully developed, it is accepted that the code relating to CoP will not have any practical effect. The steering group still thinks it right to publish these provisions, with a placeholder for when CoP should take effect in the code, so that stakeholders can give feedback on CoP as a standard of care. It is anticipated that a date will be included when the code is finalised.

3.41. When a customer is in the process of making a payment, and provides the account details of the person they want to pay, CoP will work by telling the customer whether the name of the person they have given as payee matches those account details. The code sets out that firms should then give customers help to understand the result they get from CoP, and, in particular, guidance to assist with the decision whether to proceed with the payment.

3.42. The steering group does not want CoP to interrupt legitimate payment journeys unnecessarily. To avoid this outcome, a provision has been included that firms must not implement CoP in a way that would prioritise de-risking over the proper function of CoP.

Response

3.43. The Best Practice Standards developed by UK Finance[9] are designed specifically to improve how firms respond when a customer falls victim to an APP scam.

3.44. The steering group wants to adopt and build on existing initiatives. For that reason, the code encourages firms to take up the Best Practice Standards if they have not done so already. This will:

- incentivise firms to improve their practices,
- create a level playing field for firms, and
- bring about consistent outcomes.

3.45. Firms are encouraged to take steps to delay payments or freeze funds so they can make investigations where they are concerned about APP scams. Firms have boundaries and limitations imposed on them under law and regulation, so, where relevant, the provisions include the qualification that firms do what they can within the limits of their legal and regulatory obligations.

- **Q1 Do you agree with the standards set out in the Standards for Firms?**
- **Q2 We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences - for example, whether this may enable firms to avoid reimbursing eligible victims.**

Reimbursement of Customer following an APP fraud: R1 – R4

3.46. The code reflects the proposed reimbursement principle that victims of APP scams who have met their requisite level of care should be reimbursed. This ensures consistent outcomes, a core principle of the code. It is proposed that the sending firm should administer the reimbursement payment, though this does not mean that the sending firm is necessarily liable for the cost of the reimbursement. As noted in paragraph 1.9 above, the steering group is continuing to work on identifying a solution for funding the cost of reimbursement in the scenario where all parties have met their expected levels of care, and that until that time, reimbursement would not be covered for victims in this scenario.

3.47. The code sets out a requisite level of care for customers to help protect themselves from APP scams. The treatment of customers that are vulnerable to APP scams is discussed separately, at paragraph 3.65 onward.

3.48. The steering group has been able to identify a number of matters that appear essential to good decision-making by customers. They are set out in R2(1)(a) to (g), explained below. These matters may turn on how firms behave towards their customers, including the tools they give to their customers.

3.49. The steering group has designed the provisions governing reimbursement of victims so that it is presumed that a victim will be reimbursed unless good reasons can be established that the customer should not be – in other words, the customer did not meet its requisite level of care. (However, note paragraph 1.9 about situations where firms have also met their standards.)

3.50. The provisions at R2 set out the circumstances in which a firm may choose not to give a reimbursement, which may depend on the firm's compliance with the standards under the SF provisions.

3.51. Just as firms will need to consider whether or not a particular standard under the SF provisions would have had a material effect on preventing the APP scam that took place (see above at paragraph 3.28), in establishing whether a customer should be reimbursed, firms need to consider whether what the customer did would have had a material effect in avoiding the APP scam.

9 A description of the Best Practice Standards is included in the Annex to the code

Provisions R2(1)(a) to (g)

3.52. In assessing whether a customer has met the requisite level of care and should be reimbursed, firms may take a number of matters into account. These are specifically related to steps customers should take to help protect themselves from APP scams.

3.53. R2(1)(a) and (b) - firms will have to establish compliance with the effective warnings and Confirmation of Payee standards before they can establish that a customer ignored the tools given to help them protect themselves.

- **Q3 We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.**

3.54. R2(1)(c) is there to cover payments which may have been physically made by a third party but with the consent of the customer. For example, a victim may be coached by a fraudster to hand over their PIN, or to give access to their banking app. Where this happens, if a payment is then made from the customer's account but the customer did not consent to the payment, this is likely to be treated as an unauthorised payment, outside the scope of the code. However, if the victim is tricked into handing over access to their banking app, and to consenting to the particular payment being made by the fraudster on their behalf this could be treated as an authorised payment and so would be within the code.

3.55. R2(1)(d) covers an important aspect of a customer's general responsibility: customers should try to make sure that the person they are paying is legitimate. Many scams involve sales over the internet. Whilst there are a number of well-known, 'household name' retailers operating online, the lack of face-to-face interaction on the internet can make it easier for fraudsters to trick people. We recognise that the sophistication of such purchase scams can vary.

3.56. R2(1)(e) arises as a result of so-called 'CEO frauds'. The standard method of these scams is that a communication is made, usually using a compromised (or 'hacked') email account, to an employee of a company. The email instructs the employee to make a payment on behalf of their CEO. The email is likely to be worded so as to manipulate the employee into making the payment quickly and without question.

3.57. The sophistication of these scams, in particular the use of hacked emails, makes it difficult for some small companies to protect themselves. However, microenterprises and small charities, like consumers, should help to protect themselves. It is also recognised that small companies like these are subject to a wide range of law and regulation.

3.58. As a result, it is reasonable that they should act prudently to protect their own interests. This should include that, where they have them, small companies should follow their own policies and processes. So R2(1)(e) allows firms to decide not to reimburse microenterprises and small charities who have not followed their own internal procedures.

3.59. The steering group has been made aware that there have been difficulties in the past caused when customers, who have been victims of APP scams, have been unhelpful in providing details to banks to help their investigations, or have provided incorrect or false information. We think it is right that, where customers have caused obstruction to firms and themselves by acting this way, firms could decide not to reimburse them. This is what R2(1)(f) is aimed at.

3.60. The steering group wants to be clear about conduct at which R2(1)(f) is not aimed. Some scams involve coaching a customer to 'lie' to their firm– these are known as 'impersonation frauds'. This usually involves the fraudster posing as a staff member of the customer's firm, or as a police officer, and telling the customer that their account is under attack by corrupt staff members within the firm. They go on to instruct the customer to transfer money out of the account 'under attack', to a 'safe' account which actually belongs to the fraudster. The victim is coached so that when their firm

questions the transfer, the victim avoids the questions asked because they think the firm is corrupt, so effectively lying to the firm.

3.61. This is not what is aimed at by R2(1)(f). A customer in these circumstances is likely to have had an honestly held belief that they were acting under the instructions of their own firm, or the police, in giving false answers to the firm's staff.

3.62. R2(1)(g) provides for a firm to choose not to reimburse a customer who can be shown to have acted with gross negligence. The FCA has given guidance about gross negligence, in the context of unauthorised payments, in its Approach Document[10]. Firms and customers may find this useful, and so it is set out here:

> *"Each case will need to be assessed on its merits to ascertain whether the customer has acted with "gross negligence". In line with the recitals to PSD2, we interpret "gross negligence" to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness."*

3.63. R2(2) provides an important overlay for firms when assessing whether they may choose to decline reimbursement. Because firm and customer behaviour cannot be entirely disentangled when considering whether each has done enough to prevent the APP scam in question, we think it is important to make sure that any assessment of reimbursement for a customer should not be looked at in isolation from the firm's conduct in each case.

3.64. Meeting the Standards for Firms is just one aspect of a firm's conduct that will have a bearing on how a customer is likely to conduct themselves when making payments. Under the code, firms should look at all the circumstances of a case in the round to determine whether there may be some element of their own conduct that may have caused a customer to behave the way they did when making the payment.

- **Q4 Do you agree with the steps customers should take to protect themselves?**

Customers vulnerable to APP scams: R2(3); SF1(4)

3.65. The steering group has been careful to consider the position of customers who are, or may be, considered vulnerable to APP scams.

3.66. There is a clear risk that customers less able, for whatever reason, to engage well with financial services are more likely to become victims of fraud generally, and APP scams in particular.

3.67. The steering group thinks that these customers should receive extra help to protect themselves. Because these customers are likely to be significantly less able to take steps to protect themselves, they should have different treatment in terms of reimbursement, whether or not a firm had identified a customer as vulnerable to APP scams prior to it occurring.

3.68. The code includes extra steps for firms to take for customers vulnerable to APP scams, under the Standards for Firms (SF1(4)) There are also provisions to deal with how firms should approach reimbursing these customers (R2(3)).

3.69. We think that just about everyone can become vulnerable to APP scams in some shape or form at any point in their lives, for many reasons. The steering group does intend the code to deal with cases where a victim may not appear to be vulnerable in the way it is normally thought of, for example a person living with bereavement. The question of how to define a customer that is specifically vulnerable to APP scams has been approached by making a connection between, on the one hand, how reasonable it is to expect a victim to have protected themselves from an APP scam with, on the

[10] "Payment Services and Electronic Money – Our Approach" (July 2018), para 8.221, https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf

other, their personal characteristics, the timing and method of the APP scam, and the impact suffered by them.

3.70. The steering group agreed that customers that are assessed as being vulnerable to APP scams should be reimbursed based on a case-by-case assessment. Where the customer's vulnerability means that it would not be reasonable for them to have protected themselves against that scam, or responded appropriately to any warnings given, then they should be reimbursed. This would also apply where their vulnerability meant that the APP scam would have a disproportionate impact on the customer, considering both financial and non-financial impacts. These provisions apply whether or not the firm had previously identified the customer as vulnerable prior to them becoming a victim of APP scam.

3.71. The code does not create automatic reimbursement for all customers who may be classifiable as vulnerable according to other definitions of vulnerability currently used by industry. For example, someone suffering from, say, a depressive disorder, would not automatically be reimbursed after falling victim to an APP scam. The customer's depressive disorder would clearly form part of the assessment, but it would not in itself be determinative. If the depressive condition affected the customer so that it would not be reasonable for that customer, at the time they became the victim of the particular APP scam, to have protected themselves, or responded appropriately to effective warnings and so on, then that customer should receive reimbursement. Another example might be a customer who has recently separated from a partner, or whose partner has died, may at some point become particularly vulnerable to so-called 'romance scams'. Although recently becoming single would not be determinative in itself for reimbursement purposes, if the timing and method of the romance scam, and the loss suffered as a result, meant that it wasn't reasonable to expect the customer to protect themselves, then that customer could expect reimbursement.

3.72. Regarding the extra steps firms can take, specific reference has been made to the British Standards Institution's PAS 17271 titled "Protecting customers from financial harm as a result of fraud or financial abuse: Code of Practice"[11] as something firms should consider using. This publication is currently the only published standard aimed specifically at financial services organisations which deals with recognising and protecting customers who are particularly susceptible to fraud and financial abuse.

3.73. The steering group would welcome feedback on whether the code should adopt this standard, whether there may be any issues with it, and whether there are other standards available to which the code should also refer. Feedback is also welcomed on whether the code provides sufficient incentive for firms to put additional protections in place for customers that may be vulnerable to APP scams.

3.74. Where a customer has been assessed under the code as vulnerable to the APP scam they have suffered, and firms have met all their standards, then it is proposed that the cost of the reimbursement should be funded by the customer's firm. Feedback is sought on whether this may have any unintended consequences.

- **Q5 Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?**

11 https://shop.bsigroup.com/ProductDetail?pid=000000000030330331

Timescales: R3(1)–(3)

3.75. Firms should make the decision whether or not to reimburse a customer in a timely manner. Firms should notify the customer within 15 business days[12] after that customer reported the APP scam to the firm. The draft code recognises that firms may take up to 35 business days if there are exceptional circumstances.

3.76. The steering group has chosen this timescale to align the code with the Payment Services Regulations 2017 and the complaint handling rules in the FCA's Handbook in the Dispute Resolution sourcebook (DISP)[13]. This helps to meet the core principle of delivering consistent outcomes across payment services.

- **Q6 Do you agree with the timeframe for notifying customers on the reimbursement decision?**

Access to the Financial Ombudsman Service: R4

3.77. The steering group considers that a customer who is refused reimbursement by a firm or has any other related complaint about a firm should, where eligible, be able to challenge the outcome by going to the FOS in a timely manner and having FOS review the decision. We acknowledge that there may be other reasons arising from the code about which a customer may wish to complain.

3.78. The definition of a complaint used by the FOS is set out in the FCA's Handbook.[14] In broad summary, a complaint is any oral or written expression of dissatisfaction about the provision, or failure to provide, a financial service.

3.79. Under the DISP rules, firms must handle complaints, such as those related to APP scams, within 15 business days (or 35 business days in exceptional circumstances).

3.80. There may be instances where a customer reports that they have been a victim of an APP scam, but this report does not meet the definition of a complaint. In such instances, if the customer receives a negative reimbursement decision, the customer may then make a complaint. Under the DISP rules, the FOS is required to refer that complaint back to the firm unless the time period for the firm to consider it has lapsed.

3.81. The steering group considers that all firms involved in a particular reimbursement decision should take all reasonable steps to allow a customer, where eligible, to challenge a negative reimbursement decision of the firms with the FOS if they wish to do so, as per the current complaints process[15]. A customer should not be unnecessarily delayed in doing so by the firms.

3.82. The 'early consent' rule (DISP 2.8.1R(4)) allows the FOS to start looking at a complaint as long as both the firm and the customer agree for it to do so. This rule permits the FOS to consider a complaint if, with agreement from the firm, it has informed the complainant (the customer) of the timeframe in which the firm must deal with the complaint and that the firm may resolve the complaint more quickly than the FOS, and that the customer also agrees.

[12] See the definition in the Code at DS1(2)(c) – a business day is a day on which the firm is open for business as required for the execution of a payment transaction

[13] https://www.handbook.fca.org.uk/handbook/DISP/

[14] https://www.handbook.fca.org.uk/handbook/glossary/G197.html

[15] Note that the FCA has recently consulted on extending the FOS jurisdiction to allow it to consider complaints against receiving firms: see FCA CP18/16, https://www.fca.org.uk/publication/consultation/cp18-16.pdf

Annex to the Code

3.83. The purpose of the Annex is to provide up-to-date information on practices, measures and tools that are relevant to the provisions of the code that firms can refer to. This Annex is to be kept updated on a regular basis.

- **Q7 Please provide feedback on the measures and tools in this Annex, and whether there any other measures or tools that should be included?**

4. OUTSTANDING ISSUES

How to cover the cost of reimbursement

4.1. The steering group agreed that where a customer has met its requisite level of care, they should get their money back – one of the important principles of our work has been that customers in the same circumstances have consistent outcomes.

4.2. Where one or more firms did not meet their standard of care the steering group considers that those firms should be responsible for reimbursing the customer.

4.3. However, there may be instances where a victim of an APP scam has met the requisite level of care, and so should be reimbursed, but no firm party to the code involved in the payment journey has breached any standards. In these circumstances, the steering group remains of the view that the customer should receive a reimbursement, and that reimbursement should be administered by their firm.

4.4. The steering group agreed that for a firm that has met the necessary standards to be required to bear the direct cost of reimbursement would not be compatible with the principle of consistent outcomes for firms. The steering group has therefore agreed to establish a working group to identify the source of funds for reimbursement in these cases. It will also consider how reimbursement is funded where one of the firms breached the standards but is not party to the code. The working group will be co-chaired by an industry representative and a consumer representative.

- **Q8 Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?**
- **Q9 Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?**

4.5. So far, the steering group has discussed some possible options. The working group will consider all of the available options, recognising that not all of them are within their control. It is our intention for this to be resolved in time for the implementation of a final code in early 2019.

4.6. In order to inform this working group, we would welcome feedback as part of this consultation on possible options. Some of the potential approaches that the working group will discuss in further detail are:

- Creating a contribution mechanism across all parties with an ability to prevent APP scams from occurring (for example, firms, telecoms companies, data handlers etc)
- A transaction charge on higher risk and higher value payments to be directed into a fund
- Creating different types of firm accounts with those with the ability to conduct higher risk and higher value transactions charged a fee
- Providing the ability for customers to obtain an insurance policy, either compulsory or voluntary, to insure against the no-blame scenario
- Imposing a “fine” on a firm in a ‘shared-blame’ scenario, where an equivalent amount to the value of the scam is transferred into a fund.
- Continuing to explore the possibility of legislative changes to unlock dormant funds or redirect funding from relevant regulatory fines (for example from data loss and control weaknesses).
- The possibility of a Government-run scheme similar to the Criminal Injuries Compensation Scheme.

4.7. The steering group will be able to make recommendations following the consultation period, but in the case of legislation or of a Government run scheme this is a decision for Government and not within the control of the working group.

- **Q10 What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?**

4.8. Once the mechanism is created, there will need to be a process in place to reassess the ongoing funding, based on the amount remaining and the reimbursement decisions made. It is likely, therefore, that the contribution levels would change periodically, and we would hope that they would reduce over time as the improved levels of care reduce APP scams.

4.9. Until a funding mechanism is identified, customers might not be reimbursed in the scenario where all parties have met their expected level of care under the code. Once the funding mechanism has been agreed, whether it is legally and practically possible for customers to claim from that mechanism for 'no-blame' cases occurring during the consultation period will be considered. However, this may result in 'no-blame' victims of APP scams occurring during the consultation period not receiving reimbursement.

Evidential approach

4.10. The code is clear, in R2(1), that a firm should establish certain matters before it chooses not to reimburse a customer. The steering group agrees that evidence is helpful to support firms' assessments of APP scam causes although has yet to agree what is reasonable and fair for all parties involved in the APP scam. The approach to evidence will be to provide useful exemplars to illustrate how the principles of the Code have been met because they will:

- create transparency for customers so they're aware of what will be expected of them when logging an APP scam claim
- provide greater consistency for sending and receiving firms in demonstrating compliance
- mitigate the risk of an increase of first party fraud claims potentially being made
- give firms the ability to make consistent decisions on victim cases

4.11. Because of this, the steering group has created a working group that will be co-chaired by an industry representative and a consumer group representative, which will explore how firms might approach investigating and assessing whether firms and customers have met their requisite level of care, and what potential evidence will help with this whilst taking into account each individual case on its own merit. They will be reporting back to the steering group with the aim of establishing an approach to evidence to be built into the final code in early 2019.

4.12. In order to inform the working group, early feedback is welcomed during the consultation period on reasonable and practical standards that could be used across the industry. The issues the working group will consider will include:

- Examples of tangible evidence customers can provide to demonstrate checks they completed prior to making the payment and in support of their claim
- Examples of tangible evidence sending firms can provide to demonstrate which principles they adhered to in the code
- Information the receiving firm could share with the sending firm in line with current data sharing rules, but demonstrating what actions they took in line with the code
- The outcome if one or more of the three parties are unable to provide evidence, or the evidence is inadequate to complete a balanced investigation
- Evidence the FOS would expect to receive if a case were to be escalated to them

- Suitable evidence to support claims where the customer has informed the firm that at the time of the APP scam they consider they were in a vulnerable circumstance and that this contributed to the APP scam

- **Q11 How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?**
- **Q12 Do you agree with the issues the evidential approach working group will consider?**
- **Q13 Do you recommend any other issues are considered by the evidential approach working group which are not set out above?**
- **Q14 How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?**

Governance

4.13. To remain effective, the code should adapt to changes in the ways APP scams are committed, as well as industry developments and approaches to preventing APP scams. It should also incorporate learnings from firms' investigations and assessments for reimbursement, FOS decisions, results of inter-firm disputes, and assessments of effectiveness of warnings. To achieve this, there needs to be a clear and effective governance process overseen by an appropriate body.

4.14. At this stage, the steering group has not been able to finalise the detail of who will undertake the governance function or how it will be done. There is a placeholder in the text of the code to show where the provisions setting out governance requirements will sit in the final code.

4.15. In the meantime, stakeholders are asked to contribute feedback as to who would be the most appropriate body to take on responsibility for governance of the code, and on the suggestions below for how the governance should be carried out.

4.16. The PSR has publicly stated that it does not consider it appropriate for it to take on the governance task.[16] UK Finance has also indicated that it would not be able to carry out the function due to conflicts of interest.

4.17. Other potential bodies suggested to the steering group are the NPSO and the Lending Standards Board. It has also been suggested that the steering group remains constituted and takes on the function itself.

- **Q15 Please provide views on which body would be appropriate to govern the code.**

4.18. Work will also continue to consider further the possible change process for the code. The steering group thinks that the changes to the code should be allowed on an *ad hoc* basis, to ensure that any issues or enhancements can be addressed as they arise. In addition to this, the code should undergo periodic reviews, with the first to be done one year after the code is finalised, and then every 3 years after that. During the review, the governing body should assess whether the code has been meeting its original objectives to reduce scams and increase protection of customers. The governing body will also need a process for ensuring the Annex to the code remains up to date.

4.19. The steering group are also considering how decisions about changes to the code are made. It is important that any change is properly consulted on, and these processes may vary from wide public consultation to consultation with an advisory panel consisting of a balance of affected stakeholders.

4.20. The Steering Group seeks views on these and any other relevant governance matters.

- **Q16 Do you have any feedback on how changes to the code should be made?**

16 Para 3.30, February 2018 paper (*supra,* footnote 2).

Inter-firm allocation and dispute resolution

4.21. It is proposed that the reimbursement process for customers will be administered by the victim's firm. However, in instances where the firm that has received the funds has not met the standard of care, or both firms are at fault, there will need to be a mechanism to decide how to divide the costs of reimbursement between them. A Reimbursement Flow Working Group reporting to the steering group is in place and will meet during the consultation period to continue the work to establish correct apportionment in the case of such 'shared blame', instances where one of the firms is not party to the code, and to identify an appropriate mechanism. There is a placeholder in the draft code for provisions that will cover this in the final code, once the work has been completed.

4.22. One proposal is that in shared blame scenarios, where both firms have not met the standards of care in some way, the reimbursement cost should be shared 50:50 between the two firms. This would be simple and avoid protracted discussions about levels of blame.

4.23. Open Banking has a dispute process[17] that sets out principles and a process for firms to approach an appropriate Alternative Dispute Resolution (ADR) provider to resolve issues which may be appropriate to apply to disputes under this code.

- **Q17 Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?**
- **Q18 Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the Code?**
- **Q19 What issues or risks do we need to consider when designing a dispute mechanism?**

[17] See section 7 'Mediation, Adjudication and Arbitration Best Practice Standards' of the Open Banking Dispute Management System Code of Best Practice: https://www.openbanking.org.uk/wp-content/uploads/Dispute-Management-System-Code-of-Best-Practice.pdf

5. CONSULTATION QUESTIONS

The Steering Group welcomes feedback on the code and any specific provisions including, but not limited, to those set out below.

Questions set out in the text

- Q1 Do you agree with the standards set out in the Standards for Firms
- Q2 We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences - for example, whether this may enable firms to avoid reimbursing eligible victims
- Q3 We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.
- Q4. Do you agree with the steps customers should take to protect themselves?
- Q5 Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?
- Q6 Do you agree with the timeframe for notifying customers on the reimbursement decision?
- Q7 Please provide feedback on the measures and tools in the Annex to the code, and whether there any other measures or tools that should be included?
- Q8 Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?
- Q9 Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?
- Q10 What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?
- Q11 How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?
- Q12 Do you agree with the issues the evidential approach working group will consider?
- Q13 Do you recommend any other issues are considered by the evidential approach working group which are not set out above?
- Q14 How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?
- Q15 Please provide views on which body would be appropriate to govern the code.
- Q16 Do you have any feedback on how changes to the code should be made?
- Q17 Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?
- Q18 Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the code?
- Q19 What issues or risks do we need to consider when designing a dispute mechanism?

Additional Questions

- Q20 What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?
- Q21 What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?
- Q22 Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?
- Q23 How should the effectiveness of the code be measured?

6. ANNEX: Different types of APP scam

Common types of APP scam include:

Invoice and mandate scam:	In this APP scam, the victim attempts to make a payment to settle a legitimate obligation with a legitimate payee but the fraudster manages to intervene to convince the victim to redirect the payment to the fraudster's account.
Impersonation scam – bank or police:	This occurs when a fraudster contacts the victim purporting to be from the victim's bank or the police with claims that staff are stealing money from bank accounts. The fraudster then convinces the victim to transfer money to a different account in order to safeguard it but that is in fact controlled by the fraudster.
Impersonation scam - other:	This occurs when a fraudster contacts the victim purporting to be from a service provider (such as a broadband provider) and asks the victim to make a payment. Reasons given may be to settle a fictitious fine or to cancel out a purported erroneous refund.
Purchase scam:	This occurs when the victim pays in advance for a good or a service that they never receive. These scams may involve the use of an online platform such as an auction website.
Investment scam:	In this APP scam, a fraudster convinces an investor to move their money to a fictitious fund offering significantly higher returns than they are currently receiving. Other instances of investment fraud involve carbon credits, land banks and wine scams.
Romance scam:	In this APP scam, the victim is convinced to make a payment to a person that they have met online and with whom they believe they are in a relationship.
Advance fee scam:	In this APP scam, fraudsters convince victims to pay a fee which would then result in the release of a much larger payment to the victim.