Contingent Reimbursement Model Code for Authorised Push Payment Scams

	Overarching Provisions				
OP1	In implementing and complying with this Code, Firms should act in a way which advances the following overarching objectives:				
OP1	(1)	to reduce the occurrence of APP scams;			
OP1	(2)	to increase the proportion of Customers protected from the impact of APP scams, both through reimbursement and the reduction of APP scams;			
OP1	(3)	to minimise disruption to legitimate Payment Journeys.			
OP2	Nothing in this Code should prevent any Firm, whether UK-based or not, exercising its discretion to provide ex gratia payments to a Customer should it decide to do so.				
	Note: This Code should be read in light of, and as subject to, applicable law and regulation.				

	Definitions and Scope				
DS	This Code is the Contingent Reimbursement Model Code, and references to 'Code' should be read accordingly.				
DS1	(1)	In this Code, PSRs means the Payment Services Regulations 2017 (SI 2017/752).			
DS1	(2)	The terms below, which have initial capital letters in the text of the Code, are defined as follows:			
		(a)	APP Scam		
			Authorised Push Payment scam, that is, a transfer of funds executed across Faster Payments, CHAPS or an internal book transfer, authorised by a Customer in accordance with regulation 67 of the PSRs, where		
			(i)	The Customer intended to transfer funds to another person, but was instead deceived into transferring the funds to a different person; or	
			(ii)	The Customer transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent.	
			Note 1: 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.		
			Note 2: Regulation 67 of the PSRs provides as follows: (1) A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Part only if the payer has given its consent to— (a) the execution of the payment transaction; or (b) the execution of a series of payment transactions of which that payment transaction forms part.		

			(2) Such consent—	
				(a) may be given before or, if agreed between the payer and its payment service provider, after the execution of the payment transaction;
				(b) must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider; and
				(c) may be given via the payee or a payment initiation service provider.
			(3) The payer may withdraw its consent to a payment transaction at any time before the point at which the payment order can no longer be revoked under regulation 83 (revocation of a payment order).	
			(4) Subject to regulation 83(3) to (5), the payer may withdraw its consent to the execution of a series of payment transactions at any time with the effect that any future payment transactions are not regarded as authorised for the purposes of this Part.	
			Note 3: An authorised push payment will include a payment where, as part of giving consent for a specific payment, a Customer shares access to their personal security credentials or allows access to their banking systems such as online platforms or banking apps for that payment to be made.	
		(b)	Best Practice Standards (BPS)	
			The Best Practice Standards developed by UK Finance, which in summary provide standards for firms responding to reports of scams.	
		(c)	Business day	
			As defined in regulation 2(1) of the PSRs, that is, any day on which the relevant Firm is open for business as required for the execution of a payment transaction.	
		(d)	Confirmation of Payee (CoP)	
			A solution whereby Firms provide a result showing whether the details associated with a payee account match those entered by a payer.	
		(e)	Customer	
			A payer as defined in regulation 2(1) of the PSRs, that is, a person who holds a payment account and initiates, or consents to the initiation of, a payment order from that payment account; or where there is no payment account, a person who gives a payment order, who is:	
			(i)	a Consumer, as defined in regulation 2(1) of the PSRs, that is, an individual who, in contracts for payment services to which the PSRs apply, is acting for purposes other than a trade, business or profession;
			(ii)	a Micro-enterprise, as defined in regulation 2(1) of the PSRs, that is, in summary, an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million;
			(iii)	a Charity, as defined in regulation 2(1) of the PSRs, that is, in summary, a charity with annual income of less than £1 million.

		(f)	DISP Complaint
			A complaint as defined in the FCA Handbook Glossary, as amended from time to time, which must be dealt with under the FCA's Dispute Resolution: Complaints sourcebook. In summary, this 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 which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience.
		(g)	Dispute Resolution Provider
			a natural person, independent from the parties to a dispute, appropriately skilled and experienced in providing arbitration and adjudication services in the payments and financial services field; to be read as meaning not just the identity of the person, but the entire dispute resolution service provided by that person, including procedures, fees, terms and conditions.
		(h)	Effective Warning
			A warning designed and given in accordance with the provisions in SF1(2)(a) to (e).
		(i)	Firm
			A payment services provider within the meaning of regulation 2(1) of the PSRs.
		(j)	Non-Code firm
			a payment services provider who has not volunteered to comply with the Code
		(k)	Payment Journey
			The process of bringing about an authorised payment, as defined in DS1(2)(a), including initiation of a payment order, adding a new, or amending an existing payee, all acts taken by the Customer to authorise execution of the payment, ending with the initial reception of the transaction funds in a payee account.
DS1	(3)	In this Code, 'industry standards' or 'industry guidance' should be read as meaning any relevant set of best practice standards or guidance published by a relevant recognised body, which apply at the time. Leading examples can be found in the Annex to the Practitioner Guide.	
	Scope		
DS2	(1)	This Code applies to Customers undertaking Payment Journeys as defined in DS1(2)(k):	
		(a)	between GBP-denominated UK-domiciled accounts, by any channel of push payment available to the Customer, such as in branch, on the phone, or online.
		(b)	to the point of the first reception of funds in an account held by a receiving Firm (the first generation account). Firms whose accounts are utilised in the onward transmission of APP scam funds are out of scope.

DS2	(2)	This Code does not apply to:	
		(a)	disputes relating to unauthorised payments (such as where the Customer has not consented to the payment) or other payments which are not related to an APP scam;
		(b)	private civil disputes, such as where a Customer has paid a legitimate supplier for goods, services, or digital content but has not received them, they are defective in some way, or the Customer is otherwise dissatisfied with the supplier;
		(c)	any payments completed before the coming into force of this Code.

	General Expectations of Firms		
GF	(1)	Firms should participate in coordinated general consumer education and awareness campaigns	
		(a)	Firms should take reasonable steps to raise awareness and educate Customers about APP scams and the risk of fraudsters using their accounts as 'mule accounts'. Firms should do this by undertaking their own campaigns, and/or participating in, contributing to, or promoting, campaigns undertaken by other relevant parties;
	(2)	Firms should collect and provide statistics on APP scams to their relevant trade bodies. The categories of APP scam statistics are set out in the Annex to the Practitioner Guide.	
	(3)	Firms should have processes and procedures in place to help with Customer aftercare	
		(a)	Firms should take reasonable steps so that outcomes for Customers who have been victims of an APP scam, whether they have been reimbursed or not, go further and include, for example, further education measures, referrals for advice, and other tools enabling Customers to protect themselves. Leading examples can be found in the Annex to the Practitioner Guide.

	Standards for Firms				
SF	These provisions set out the standards that Firms should meet. If Firms fail to meet these standards, they may be responsible for meeting the cost of reimbursing, in accordance with R1, a Customer who has fallen victim to an APP scam. The assessment of whether a Firm has met a standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the APP scam that took place.				
	Payment Journey – sending Firm				
SF1	Sending Firms should take reasonable steps to protect their Customers from APP scams. This should include procedures to detect, prevent and respond to APP scams. Procedures should provide a greater level of protection for Customers who are considered vulnerable to APP scams.				
		Detection			
SF1	(1)	Firms should take appropriate action to identify Customers and payment authorisations that run a higher risk of being associated with an APP scam			
		(a)	Firms should establish transactional data and customer behaviour analytics incorporating, where appropriate, the use of fraud data and typologies to identify payments that are at higher risk of being an APP scam.		
		(b)	Firms should train their employees on how to identify indicators of circumstances around, and leading to, transactions that are at higher risk of facilitating APP scams		
		Prevention			
SF1	(2)	Where Firms identify APP scam risks in a Payment Journey, they should take reasonable steps to provide their Customers with Effective Warnings, which should include appropriate actions for those Customers to take to protect themselves from APP scams.			
		(a)	Firms should take reasonable steps to make their Customers aware of general actions that could be taken to reduce the risk of falling victim to an APP scam		
		(b)	Where the Firm identifies an APP scam risk, it should provide Effective Warnings to customers. This may occur in one or more of the following:		
			(i)	when setting up a new payee	
			(ii)	when amending an existing payee; and/or	
			(iii)	during the Payment Journey, including immediately before the Customer authorises the payment, before the Customer's account is debited	
		(c)	Effective Warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the Customer is initiating the payment instructions		
		(d)	Effective Warnings should enable the Customer to understand what actions they need to take to address the risk, such as more appropriate payment		

			methods which may have additional protections, and the consequences of not doing so.	
		(e)	As a minimum, Effective Warnings should meet the following criteria	
			(i)	Understandable – in plain language, intelligible and meaningful to the Customer
			(ii)	Clear - in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's Principles for Businesses
			(iii)	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;
			(iv)	Timely – given at points in the Payment Journey most likely to have impact on the Customer's decision-making;
			(v)	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.
SF1	(3)	From [DATE TBC], Firms should implement Confirmation of Payee in a way that the Customer can understand, and respond to it, including by:		
		(a)	taking reasonable steps to ensure that the originating Customer receives appropriate guidance that the Customer can understand at the relevant stage of the Payment Journey to assist with the decision as to whether to proceed	
		(b)	helping the Customer to be able to understand what actions they need to take to address the risk	
SF1	(4)	Firms should apply additional measures to protect Customers that are, or may be, vulnerable to APP scams under the provisions at R2(3).		
		(a)	Firms should take steps to identify Customers who are or might be vulnerable to APP scams under the provisions at R2(3)	
		(b)	Firms should implement measures and other tools to reduce the likelihood of such Customers becoming victims, or repeat victims, of APP scams. Leading examples can be found in the Annex to the Practitioner Guide.	
		(c)	Firms should include consideration of relevant industry standards, for example the BSI PAS 17271	
		Response		
SF1	(5)	Where a Firm has sufficient concern that a payment may be an APP scam, it should take appropriate action to delay the payment while it investigates		
		(a)	Where Firms have concerns, Firms should intervene on a risk-based approach to delay execution of the payment authorisation to the extent possible within the limits of law and regulation, taking reasonable steps to communicate with the originating Customer	
SF1	(6)	Where an APP scam is reported to a Firm, the sending Firm should notify any UK receiving Firms in accordance with the procedure and timeframes set out in the Best Practice Standards		

		(a)	Firms should notify the receiving Firms within the timeframes, and in the manner, set out in the Best Practice Standards
	Payment Journey – receiving Firms		
SF2	Receiving Firms should take reasonable steps to prevent accounts from being used to launder the proceeds of APP scams. This should include procedures to prevent, detect and respond to the receipt of funds from APP scams. Where the receiving Firm identifies funds where there are concerns that they may be the proceeds of an APP scam, it should freeze the funds and respond in a timely manner.		
		Prevention	
SF2	(1)	Firms must take reasonable steps to prevent accounts being opened for criminal purposes	
		(a)	Firms must open accounts in line with legal and regulatory requirements on Customer Due Diligence (CDD) using identification processes and documentation that are recommended by industry guidance
		(b)	Firms should use available shared intelligence sources and industry fraud databases to screen Customer accounts and apply industry typologies to identify accounts at higher risk of being used by criminals.
SF2	(2)	From [DATE TBC], Firms should implement Confirmation of Payee in a way so that the Customer can understand, and respond to it	
		Detection	
SF2	(3)	Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP scam funds.	
		(a)	Firms should establish transactional data and customer behaviour analytics incorporating, where appropriate, the use of fraud data and typologies to identify payments into accounts that are at higher risk of being an APP scam
		(b)	Firms should train their employees on how to identify indicators of circumstances around, and leading to, transactions that are at higher risk of facilitating APP scams
		Response	
SF2	(4)	Following notification of concerns about an account or funds at a receiving Firm, the receiving Firm should respond in accordance with the procedures set out in the Best Practice Standards.	
		(a)	Receiving Firm should respond to the sending Firm appropriately within the timeframes, and in the manner, set out in the Best Practice Standards
SF2	(5)	On identifying funds where there are concerns that they may be the proceeds of an APP scam, Firms must take reasonable steps to freeze the funds and, when appropriate, should repatriate them to the Customer's Firm in accordance with the procedures set out in the Best Practice Standards.	
		(a)	Firms must freeze any remaining funds and should take steps to repatriate the funds to the Customer's Firm, to the extent possible within the limits of law and regulation.

	Reimbursement of Customer following an APP scam				
	Principle				
R1	Subject to R2, when a Customer has been the victim of an APP scam Firms should reimburse the Customer				
	Exceptions				
R2	(1)	A Firm may choose not to reimburse a Customer if it can establish any of the following matters in (a) to (e). The assessment of whether these matters can be established should involve consideration of whether they would have had a material effect on preventing the APP scam that took place.			
		(a)	The Customer ignored Effective Warnings, given by a Firm in compliance with SF1(2), by failing to take appropriate action in response to such an Effective Warning given in any of the following:		
			(i)	when setting up a new payee;	
			(ii)	when amending an existing payee, and/ or	
			(iii)	immediately before making the payment	
		(b)	From [DATE TBC], the Customer did not take appropriate actions following a clear negative Confirmation of Payee result, where the Firm complied with SF1(3) or SF2(2), and those actions would, in the circumstances, have been effective in preventing the APP scam;		
		(c)	In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that:		
			(i)	the payee was the person the Customer was expecting to pay;	
			(ii)	the payment was for genuine goods or services; and/or	
			(iii)	the person or business with whom they transacted was legitimate.	
		(d)	Where the Customer is a Micro-enterprise or Charity, it did not follow its own internal procedures for approval of payments, and those procedures would have been effective in preventing the APP scam;		
		(e)	The Customer has been grossly negligent. For the avoidance of doubt the provisions of R2(1)(a)-(d) should not be taken to define gross negligence in this context.		
R2	(2)	In assessing whether a Customer should be reimbursed or not, Firms should consider			
		(a)	whether the acts or omissions of Firms involved in trying to meet the Standards for Firms may have impeded the Customer's ability to avoid falling victim to the APP scam		
		(b)	whether, during the process of assessing whether the Customer should be reimbursed, the Customer has acted dishonestly or obstructively in a material respect		

	Customers Vulnerable to APP scams		
R2	(3)	A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered. This should be assessed on a case-by-case basis. In these circumstances, the Customer should be reimbursed notwithstanding the provisions in R2(1), and whether or not the Firm had previously identified the Customer as vulnerable. Factors to consider include:	
		(a)	All Customers can be vulnerable to APP scams and vulnerability is dynamic. The reasons for dynamics of vulnerability may include: the personal circumstances of the Customer; the timing and nature of the APP scam itself; the capacity the Customer had to protect themselves; and the impact of the APP scam on that Customer
		(b)	A Customer's personal circumstances which lead to vulnerability are varied, may be temporary or permanent, and may vary in severity over time
		(c)	APP scams may include long-running APP scams or in the moment APP scams.
		(d)	The capacity of a Customer to protect themselves includes their knowledge, skills and capability in engaging with financial services and systems, and the effectiveness of tools made available to them by Firms.
		(e)	The impact of the APP scam includes the extent to which the Customer is disproportionately affected by the APP scam, both financially and non-financially.
	Claims timeline and complaints		
R3	(1)	Firms should make the decision as to whether or not to reimburse a Customer without undue delay, and in any event no later than 15 Business days after the day on which the Customer reported the APP scam.	
		(a)	In exceptional cases, that period can be extended provided the Firm informs the Customer of the delay and the reasons for it, and the date by which the decision will be made
		(b)	The date in (a) should not be more than 35 Business days after the day on which the Customer reported becoming the victim of an APP scam.
	(2)	Once a decision to reimburse has been made, the Firm of whom the APP scam victim is the Customer should administer the payment of the reimbursement to their Customer without delay. Reimbursement should not be delayed in any way by any question of the allocation of the cost of the reimbursement.	
R4	(1)	On completion of a reimbursement decision, within the written notification to the Customer, the Firm should provide guidance advising the Customer of their right to make a DISP Complaint to both the sending and receiving Firm and the process to follow should they wish to do so.	

	(2)	If the Firm invokes R3(1)(a), within the written notification to the Customer, the Firm should provide an explanation for the additional time required. The Firm should also advise the Customer of their right to make a DISP Complaint to both the sending and receiving Firm and the process to follow should they wish to do so.	
	(3)	Following notification of a reimbursement decision, if the Customer is dissatisfied with the outcome and wishes to raise a DISP complaint, Firms should ensure that conclusion of the customer's case is not unnecessarily delayed and allow them to raise a case with the Financial Ombudsman Service should they wish/need to do so. The firm should either:	
		(a)	resolve the DISP Complaint within a faster, expedited timescale, wherever possible within 15 Business days of the DISP complaint being made, or in exceptional cases within 35 Business days provided the Firm informs the Customer of the delay and the reasons for it, and the date by which the decision will be made; or
		(b)	provide early consent to the case going to the FOS, under the provisions in the FCA Handbook at DISP 2.8.1R(4).
	(4)	Upon receipt of a DISP Complaint against both the sending and the receiving Firm, the sending Firm must forward the details onto the receiving Firm promptly. Upon receipt of the DISP Complaint, the DISP timeline will begin for both Firms.	

	Allocation		
ALL1	The following provisions apply when a decision is taken on reimbursement of a Customer as a result of R1. Note that one instance of an APP scam may comprise more than one Payment Journey – Firms should approach the allocation of the cost of reimbursement on the basis of each individual Payment Journey.		
ALL2	When a Customer has been reimbursed, Firms involved in each relevant Payment Journey should make all efforts to agree unanimously the allocation of the cost of reimbursement between them.		
ALL3	(1)	Firms should use the following allocation principles as best practice guidance	
		(a)	Where both Firms have breached SF, then each should contribute 50% of the cost of reimbursement;
		(b)	Where one Firm only has breached SF, that Firm should meet 100% of the cost of reimbursement

	(2)	Where neither Firm involved in the relevant Payment Journey has breached any provision of SF, the Customer's Firm who has administered the reimbursement should apply to [the no-blame fund] to recoup the cost of the reimbursement.		
	(3)	Where a Customer should receive reimbursement under R1, but one party in the relevant Payment Journey is a Non-Code firm:		
		(a)	The Customer's Firm shall make best endeavours to contact the Non-Code firms and seek their cooperation in bearing the costs of reimbursement as per ALL2 and ALL3(1).	
		(b)	Where the receiving firm is a Non-Code firm and refuses to bear any cost of reimbursement, the Customer's Firm should:	
			(i)	advance to the Customer 100% of the monies for reimbursement,
			(ii)	Apply to [the no-blame fund] to recover the reimbursement monies, and
			(iii)	support the Customer to make DISP complaints against the Non-Code firms involved to recover the outstanding monies
	(4)	All relevant Firms should keep a written record of the allocation agreement, attested by all parties, and retain that record for at least 6 years.		
ALL4	If unanimous agreement under this section has not been reached after 15 Business days following the day on which a decision on reimbursement to the Customer was made, the provisions in DR will apply.			

	DISPUTE RESOLUTION	
DR1	(1)	Where, in accordance with ALL4, Firms are unable to reach unanimous agreement regarding allocation, Firms should resolve the dispute using a method of alternative dispute resolution, in accordance with the following provisions.
	(2)	The Firm wishing to use alternative dispute resolution must notify the other Firms involved that it intends to refer the matter to a dispute resolution process.
	(3)	Unless unanimous agreement has been reached in the meantime, 5 business days after receipt of the notice of intention to refer, the dispute resolution process should be commenced by the case handler.
	(4)	Firms should seek to use adjudication, unless the nature of the dispute is such that all parties agree that arbitration is the better option.
DR2	(1)	All Firms party to the dispute should follow the principles set out below:

		(a)	The sending Firm should act as the case handler for the dispute resolution process	
		(b)	(i)	Subject to (ii), the sending Firm should propose the Dispute Resolution Provider to be used;
			(ii)	If all parties do not agree with the sending Firm's proposition without delay, or in any event within [5 Business] days of the proposition being communicated, DR3 will apply
		(c)	(i)	The sending Firm should draft a notice of dispute for resolution, including a summary of the facts and issues requiring resolution
			(ii)	The draft notice must be sent to the other parties without delay, and in any event within [5 Business] days of the Dispute Resolution Provider being appointed
			(iii)	All parties should agree the content of the draft notice without delay, or in any event within [5 Business] days of receipt, after which the sending Firm should promptly provide the notice to the Dispute Resolution Provider
		(d)	Firms should	
			(i)	Adhere to the procedure for the dispute resolution proceedings as set out by the Dispute Resolution Provider; and
			(ii)	be bound by the decision of the Dispute Resolution Provider
		(e)	Firms should bear in equal proportions the reasonable costs of the Dispute Resolution Provider in providing the dispute resolution process	
		(f)	In all other respects, each Firm should bear its own costs	
		(g)	All Firms should ensure:	
			(i)	All parties to the dispute are treated fairly;
			(ii)	All information exchanged electronically is done so with appropriate security measures;
			(iii)	Appropriate records of the dispute resolution process are made and retained
	(2)	The case handler should have the following responsibilities:		
		(a)	referring the dispute to a Dispute Resolution Provider,	

		(b)	Acting as a single point of contact throughout the dispute resolution process
		(c)	obtaining from the Dispute Resolution Provider a written declaration of any matter that may, or may be seen to, compromise that provider's independence, prior to the appointment of the provider being made
DR3	Where the parties to the dispute cannot agree on a Dispute Resolution Provider then the Centre for Effective Dispute Resolution, www.cedr.com (CEDR) should be used.		