Contingent Reimbursement Model

	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 fraud;
OP1	(2)	to increase the proportion of Customers protected from the impact of APP fraud, both through reimbursement and the reduction of APP fraud;
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 Fraud		
			Authorised Push Payment Fraud, 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.		
		(b)	Best Practice Standards (BPS)		

			The Best Practice Standards developed by UK Finance, which in summary provide standards for firms responding to reports of fraud, and for apportioning costs of reimbursements among firms involved in transactions related to an APP fraud.	
		(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 Microenterprise, 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)	Effective Warning	
			A warning designed and given in accordance with the provisions in SF1(2)(a) to (e).	
		(g)	Firm	
			A payment services provider within the meaning of regulation 2(1) of the PSRs.	
		(h)	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 this Code.		
	Scope			

DS2	(1)	This Code applies to Customers undertaking Payment Journeys as defined in DS1(2)(h):	
		(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 by a receiving Firm (the first generation account). Firms whose accounts are utilised in the onward transmission of APP fraud 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 fraud;
		(b)	commercial disputes, such as where a Customer has paid a legitimate supplier for goods, services, or digital content but has not received them, or they are defective in some way;
		(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 fraud 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 fraud to their relevant trade bodies. The categories of APP fraud statistics are set out in the Annex to this Code.	
	(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 fraud cover more than simple reimbursement, 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 this Code.

	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 APP fraud. 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 fraud that took place.				
	Payment Journey – sending Firm				
SF1	Sending Firms should take reasonable steps to protect their Customers from APP fraud. This should include procedures to detect, prevent and respond to APP fraud. Procedures should provide a greater level of protection for Customers who are considered vulnerable to APP fraud.				
		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 fraud			
		(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 fraud.		
		(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 fraud		
		Prevention			
SF1	(2)	Where Firms identify APP fraud 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 fraud.			
		(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 fraud		
		(b)	Where the Firm identifies an APP fraud 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 fraud risk indicators and any specific APP fraud 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 fraud 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 fraud 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 fraud under the provisions at R2(3).		
		(a)	Firms should take steps to identify Customers who are or might be vulnerable to APP fraud 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 fraud. Leading examples can be found in the Annex to this Code.	
		(c)	Firms should include consideration of relevant industry standards, in particular the BSI PAS 17271	
		Response		
SF1	(5)	Where a Firm has sufficient concern that a payment may be an APP fraud, 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 fraud 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 fraud. This should include procedures to prevent, detect and respond to the receipt of funds from APP fraud. Where the receiving Firm identifies funds where there are concerns that they may be the proceeds of an APP fraud, it should freeze the funds and respond in a timely manner.		
		Prevent	
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 subject to independent verification or otherwise 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	
		(a)	Firms should not use Confirmation of Payee as a means to reduce their risk of potential liability for funding the cost of a reimbursement to a Customer in a way that would be likely to prejudice or unduly disrupt legitimate payments.
		Detect	
SF2	(3)	Firms must take reasonable steps to detect accounts which may be, or are being, used to receive APP fraud 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 fraud
		(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 fraud
		Respond	
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 implement the Best Practice Standards and respond to the sending Firm appropriately

SF2	(5)	On identifying funds where there are concerns that they may be the proceeds of an APP fraud, Firms must take reasonable steps to freeze the funds and, when appropriate, should repatriate them to the Customer via 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, via the sending Firm, to the extent possible within the limits of law and regulation.

	Reimbursement of Customer following an APP fraud				
R1	Subject to R2, when a Customer has been the victim of an APP fraud, Firms should reimburse the Customer				
R2	(1)	A Firm may choose not to reimburse a Customer if it can establish any of the following matters in (a) to (g). 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 fraud 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)	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 fraud;		
		(c)	Recklessly sharing access to their personal security credentials or allowing access to their banking systems such as online platforms or banking apps;		
		(d)	Failing to take reasonable steps to satisfy themselves that a payee was the person the Customer was expecting to pay;		
		(e)	Where the Customer is a Microenterprise 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 fraud;		
		(f)	The Customer has not acted openly and honestly in their dealings with their Firm during the process of the Firm establishing whether the Customer should be reimbursed;		
		(g)	The Customer has been grossly negligent.		
R2	(2)	In assessing whether a Customer should be reimbursed or not, Firms should consider 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 fraud.			
R2	(3)	A Customer is vulnerable to APP fraud if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP fraud, against that particular APP fraud, 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 fraud 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 fraud		

			itself; the capacity the Customer had to protect themselves; and the impact of the fraud 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 fraud may include long-running APP fraud or in the moment APP fraud.
		(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 fraud includes the extent to which the Customer is disproportionately affected by the APP fraud, both financially and non-financially.
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 fraud.	
		(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 fraud.
	(2)	Once a decision to reimburse has been made, the Firm of whom the APP fraud 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 apportionment of the cost of the reimbursement.	
R4	Where a Customer has received a negative reimbursement decision, all the Firms involved will take all reasonable steps to enable a Customer who is eligible and wishes to do so, to commence immediately the process of challenging that decision with the Financial Ombudsman Service.		

	Apportionment and Dispute Resolution [PLACEHOLDER]

	Governance [PLACEHOLDER]

ANNEX

Table 1: APP fraud prevention and response measures and tools currently available or being implemented
Consumer education and awareness
Take Five to Stop Fraud: the coordinated national campaign to raise awareness about financial crime, including APP fraud. Friends Against Scams: campaign to raise awareness to look out for those in the community that may be particularly susceptible to APP fraud. FCA scam smart.
The Banking Protocol
A protocol for bank cashiers in branch that identify transactions that look unusual. The protocol calls for cashiers to ask further questions of the customer, and to call police on 999 if they suspect a crime in action. Police will attend to the customer in branch to discuss the situation, help stop any fraud payments being made and arrest any suspects nearby.
Best practice standards for responding to APP fraud claims (APP claim reporting standards)
These are a set of standards and timeframes that sending and receiving Firms follow when processing an APP fraud claim. This includes standards for engagement with the customer.
Confirmation of Payee
A solution which allow customers to verify that they are paying the person they intended before transferring the money. The payer will be notified that the details don't match the name they've entered and can choose to not proceed with the payment.
Network-level transaction data analytics
Firms have systems and capabilities for analysing their internal transactions. Network-level transaction data analytics is a new solution that analyses network-wide interbank payment transaction data to help identify money mule accounts that are used to perpetrate APP and other payment fraud, and the flow of funds related to these crimes to help with more efficient recovery of funds.
Guidelines for identity verification, authentication and risk assessment
Best practice guidelines for Firms to use when verifying a user's identity.
Consented standardised information set data sharing (previously known as Trusted 'Know Your Customer' Data Sharing)
Standards and rules for a data sharing framework that Firms (and possibly other participants) will use to store and share KYC data, enable more efficient and cost-effective sharing of information to apply in KYC checks. This is initially focused on current account openings for business customers.
Economic crime information sharing (previously known as Financial Crime Data and Information Sharing)
A more effective economic crime data and information sharing framework between Firms that will help them detect and prevent financial crime activity, such as money mule accounts used to perpetrate APP fraud.

Table 2: Measures and other tools for addressing consumer vulnerability
British Institute of Standards' PAS 17271: Protecting customers from financial harm as a result of fraud or financial abuse – Code of practice
Sets out a code of practice for Firms to follow on protecting consumers from financial harm. This includes practices for Firms to: • train staff on vulnerability and to be able to identify customers who may be particularly susceptible to fraud. • take actions to reduce the risk of harm for those who may be susceptible to fraud • respond to an incident of fraud and provide appropriate support to the victim
Payment authorisation deferral
Firms could allow customers that are more susceptible to defer the authorisation of an outgoing payment for a period of up to 72 hours after the instructions are issued, and make them aware they offer this. It effectively delays the outgoing payment to allow for additional time for the customer to come out of the 'hot state' created by the criminal, to speak to a trusted friend or relative about the transaction, and for further investigation.
Credit flags for customers with lack of capacity
Individuals can be registered as not having capacity and a flag placed on their account. With this flag, if credit is applied for in their name, it will be refused and a notification delivered to the person who registered the individual.

Table 3: Current practice on APP fraud statistics
APP fraud statistics are collected and provided on a monthly basis to UK Finance, who in turn publishes these on a six-monthly basis.
The following categories of APP fraud statistics are collected: • Volume (number of cases, number of victims) • Value • Type of victim (consumer; business) • APP fraud type (Impersonation scam: Police/Bank staff; Impersonation scam: Other; Invoice and mandate scam; Purchase scam; CEO Fraud; Advance fee scam; Investment scam; Romance scam) • Payment system used • Payment channel (online, in branch, telephone) • Time taken to complete the various steps of the APP fraud investigation