BCLP. Client Intelligent

Insights

AUTHORISED PUSH PAYMENT SCAMS - THE VOLUNTARY CODE

May 31, 2019

> Following a super-complaint by Which?, the Payment System Regulator ("PSR") investigated and consulted in 2016 and 2017 on whether and how victims of authorised push payment ("APP") scams should be better protected. Subsequently, the PSR decided to introduce a Contingent Reimbursement Model ("CRM") and concluded that the best way to implement the CRM was by way of an industry voluntary code. The PSR established, in March 2018, the Authorised Push Payments Scams Steering Group ("Steering Group") to develop the voluntary code. On 28 February 2019, the Steering Group published the final code - Contingent Reimbursement Model Code for Authorised Push Payment Scams ("CRM Code"). The CRM Code entered into force on 28 May 2019.

As the CRM Code is voluntary in nature, the "in-force" date essentially means that payment service providers ("PSPs") which sign up to it should deal with APP scams in accordance with the code from that date (see further discussion below). The actual administration and governance of the CRM Code will be handed over from the Steering Group to the Lending Standards Board ("LSB") from 1 July 2019. The LSB has published on its website a formal version of the CRM Code and some further information on the code (including a FAQ). The Steering Group will continue to exist and act as an adviser to the LSB.

The CRM Code is expressed to apply to all PSPs as defined in the Payment Services Regulations 2017 ("PSR2017"). However, the current wording does not anticipate its application to payment initiation service providers ("PISPs"). The Steering Group states in its feedback on the consultation that it is working with the Open Banking Implementation Entity and the LSB on an approach to how the CRM Code will apply to PISPs.

Scope of the code

The CRM code applies only to payment transactions that meet certain specified parameters which are:

- The transaction must be an "Authorised Push Payment scam" and it must be executed across Faster Payments or CHAPS.

As the term indicates, the transaction must be "authorised" by the payer in accordance with the relevant requirements under the PSR2017 (i.e. the payer giving consent to the sending PSP to execute the transaction). Unauthorised transactions are outside the scope (e.g. where the fraudster stole the security credentials and used them, without the victim knowing, to make payments).

The term "scam" effectively means that the victim was tricked into authorising the payment. There are two scenarios: where the victim intended to transfer funds to X but was deceived into transferring the funds to Y; or where the victim transferred funds to X for what they believed were legitimate purposes but which were in fact fraudulent (e.g. an impersonation scam).

- The transaction must be between GBP-denominated UK domestic accounts.

  This means that if the receiving account (i.e. the fraudster's account) is in a foreign country, then it will fall outside the scope; similarly, if the transaction is in non-GBP currency (e.g. euro), that will also fall outside the scope.

- The payer (i.e. victim) must be a consumer, a micro-enterprise or a small charity.

  These terms are the same as those defined in the PSR2017. In summary, a "consumer" is an individual who is not acting for business purposes; a "micro-enterprise" is an enterprise with fewer than 10 staff and whose annual turnover/balance sheet total does not exceed EUR2 million; a "charity" is one with annual income of less than £1 million.

- The transaction is between the victim's account and the first receiving account (referred to as a "first generation account").

  This means that the CRM Code applies to only the sending PSP that acts for the payer (i.e. victim) and the receiving PSP that acts for the payee (i.e. fraudster) and first receives the funds. That is, if the fraudster subsequently transfers the funds from the first generation account to other account(s), then the down-stream PSPs where those further accounts are held have no responsibilities towards the victim under the CRM Code.

  Note that those down-stream PSPs may still need to cooperate with the first receiving PSP under the PSR2017. Further, the Financial Conduct Authority ("FCA") at the end of 2018 made new rules to allow consumers to raise complaints relating to APP fraud with the Financial Ombudsman Service ("FOS") against the receiving PSP (here, the PSP whose customer is the fraudster receiving the funds). These new rules have been in force since January 2019. Therefore, notwithstanding the first generation account provisions under the CRM Code, the victim may still be able to raise a complaint with the FOS against one of such down-stream PSPs under the new FCA rules. This is because the new FCA rules refer to a PSP that "is (or was) **involved** in the transfer of the funds" (emphasis added) and the FCA rules are intended to work "even in the absence of the CRM code". However, it is not entirely clear whether and how

the victim would obtain any additional protection from the FOS in such circumstances, given that the FOS (when dealing with such complaints) is expected to take into account the CRM Code which provides such down-stream PSPs are not responsible.

Conduct standards under the code

The CRM Code sets out standards of conduct for both the sending PSP and the receiving PSP (i.e. the receiving PSP where the first generation account is held). These standards cover "detection", "prevention" and "response", which also distinguish between a sending PSP and a receiving PSP. Understandably, the standards on the sending PSP are more extensive than those on the receiving PSP. In summary, the sending PSP should take reasonable steps to detect APP scams and subsequently should send "effective warning" to the potential victim about the risk and what the victim should do to protect themselves. PSPs should also delay processing of the relevant transaction (for sending PSPs) or freeze the funds (for receiving PSPs).

The industry in the consultation process raised concerns with respect to the potential conflicts between these standards and the relevant legal/regulatory requirements. For example, the PSR2017 has specific time limits on transaction processing for both sending PSPs and receiving PSPs. The Steering Group states in its response that the CRM Code expects PSPs to take action within the existing legal and regulatory constraints including PSR2017.

The CRM Code also puts reliance in a number places on the Best Practice Standards issued by UK Finance on APP scams (e.g. the sending PSP should notify the receiving PSP of a potential APP scam in accordance with the procedures in those Best Practice Standards). However, these Best Practice Standards, for the time being, are available only to UK Finance members. The Steering Group notes that UK Finance is in the process of making them available to non-members as well.

Reimbursing victims

The default position under the CRM Code is that the victim of an APP scam should be reimbursed, which is the primary purpose of the code.

There are specific circumstances that are carved out from this general principle, which are referred to as "exceptions". That is, a PSP "may choose not to reimburse" a victim under any of those exceptions. The main exceptions are, in summary:

- The victim ignored warnings given in compliance with the CRM Code.
- The victim made the payment without a reasonable basis for believing that the transaction was legitimate.

  This effectively refers to the situation where the victim should have realised that the payment was a scam. However, this will need to be assessed taking into account "all the circumstances

at the time of the payment", particularly the characteristics of the victim and the complexity and sophistication of the scam. In other words, this is the level of care expected of the victim.

During the consultation, there was tension between the industry and the consumer groups. The industry wished to have more clarity on the level of care that consumers should comply with, whereas the consumer groups wished to have such requirements removed completely. The Steering Group acknowledged that it was difficult to find a compromise. As a result, the Steering Group (in addition to some drafting clarifications in the final code) proposed a long term action plan. The action plan includes steps such as: consumer education and awareness campaigns to inform consumers of the steps they should themselves take (for these purposes, the LSB has published a guide and a FAQ pack aimed at consumers); and a practitioner guide (for the PSPs) which will include explanations and examples to show when a customer should be regarded as not having a reasonable basis for belief (the guide is still being developed by the LSB and the Steering Group). Other steps include review and amendment of the code and how the FOS would interpret 'reasonableness' in this context.

- Where the victim is an entity (i.e. a micro-enterprise or small charity), it did not follow its own internal payment procedures.
- The victim has been grossly negligent in making the payment.
- Note that the actions of the victim under the other exceptions should not be taken to indicate gross negligence for this purpose.

During the consultation process, the industry wished to have "gross negligence" defined. The Steering Group declined to do so on the ground that this is a legal concept for the courts. The Steering Group, however, explained it (in its consultation paper and the final feedback on the consultation) by quoting the FCA's view in the FCA's Approach Document for Payment Services and Electronic Money.

The FCA states therein that "[e]ach 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."

Accordingly, there may be difficulties for PSPs to rely on this exception in practice.

Note that if a victim is assessed as being vulnerable to APP scams, then the victim should be reimbursed notwithstanding that the victim may fall within one of the exceptions.

The CRM Code lists a number of (non-exhaustive) factors that should be considered in the vulnerability assessment, including the victim's personal circumstances, their knowledge, skills and capabilities in engaging with financial services and the (financial or non-financial) impact of the

scam on the particular victim. The starting position is that all customers can be vulnerable for these purposes and vulnerability is dynamic.

Concerns were raised in the consultation process that smaller PSPs may have difficulties in conducting the vulnerability assessment as they (contrasting with big banks) tend to hold less data on customers. However, the Steering Group concludes that the requirements are appropriate and notes that the practitioner guide (which is still being developed) would provide helpful guidance and examples on how the assessment should be conducted. The Steering Group also points to the "Code of Practice - Protecting customers from financial harm as a result of fraud or financial abuse" published by the British Standards Institute as an example of industry guidance on vulnerability.

The Steering Group further notes that where a PSP after the vulnerability assessment decides not to reimburse a customer, that customer would be able to look to the FOS to challenge that conclusion. This statement appears to add even more uncertainty to the vulnerability assessment. It remains to be seen how PSPs should carry out such assessment in practice without the FOS overturning it in a challenge.

Allocation of cost

The CRM Code sets out a mechanism whereby the sending PSP and the receiving PSP should allocate between themselves the cost of reimbursing the victim of an APP scam. This may be summarised in four allocation scenarios:

- PSPs at fault (but victim not at fault)If both the sending PSP and the receiving PSP are at fault, then they each should contribute 50% of the reimbursement.

If one PSP is at fault (e.g. having breached one or more conduct standards), then that PSP is liable for 100% of the reimbursement.

If both the sending PSP and the receiving PSP are at fault, then they each should contribute 50% of the reimbursement.

- Customer at fault

  If both the sending PSP and the receiving PSP are also at fault, then all three parties will accept an equal share of liability. In other words, each PSP contributes 33% of the reimbursement, with the victim receiving a 66% reimbursement.

  If either the sending PSP or the receiving PSP is also at fault, then the victim receives a 50% reimbursement from that PSP.

- No one at fault

This is where each of the sending PSP, the receiving PSP and the victim has met their requisite level of care. In such no-blame scenarios, the victim's PSP (i.e. the sending PSP) should 'administer' (i.e. no liability) the reimbursement and then re-coup the cost from a pooling fund.

This pooling fund is now temporarily referred to as "[the no-blame fund]". The Steering Group is still in the process of agreeing a long-term funding arrangement for this no-blame fund with the industry. The long-term funding mechanism is expected to be introduced for January 2020. According to the website of UK Finance, the temporary fund from the period from 28 May till the end of 2019 has been established by some of the major UK banks (including Barclays, HSBC, Lloyds, Nationwide and RBS) which are also the current PSPs that have signed up to the CRM Code.

- Receiving PSP outside code

If the receiving PSP has not adopted the CRM Code (given it is voluntary), the sending PSP should first use its best endeavours to seek cooperation in terms of bearing the cost of reimbursement in accordance with the relevant scenario (see above). If the receiving PSP refuses, then the sending PSP should reimburse 100% the victim and then apply to recoup the cost from the no-blame fund. The sending PSP should also support the victim in making a complaint to the FOS against the receiving PSP.

However, the CRM Code does not have provisions on the situation where the sending PSP has not adopted the CRM Code. As the sending PSP is the first "port of call" for the victim and is the one that administers the reimbursement, it is not clear what and how victims should proceed under these circumstances.

Another point that is worth noting is that there is no degree of fault. The allocation provisions simply refer to breaching of the standards of conduct under the code (see above), although there is a dispute resolution mechanism where the PSPs fail to reach an agreement on allocation.

Concluding remark

As noted above, the CRM Code is expressed as a voluntary code and as such it is up to each PSP as regards whether to follow the code or not. However, the Steering Group notes that "it is anticipated that the Financial Ombudsman Service will consider taking the code into account as a relevant consideration when handling complaints against [PSPs] arising from APP fraud".

Further, it is understood that the FCA expects PSPs to implement the code consistently and that arbitrary interpretation may potentially give rise to an FCA enforcement action notwithstanding the CRM Code being voluntary. It is also understood that the PSR does not exclude the introduction of legislation if voluntary adoption does not progress satisfactorily over time. The Steering Group itself also noted that it "expects…the voluntary nature…will be reviewed in the longer term".

Given these and the current focus on addressing APP scams, we would recommend PSPs to consider carefully the CRM Code and the potential risks of not adopting it (despite of it being voluntary).

MEET THE TEAM

Samantha Paul

London

samantha.paul@bclplaw.com
+44 (0) 20 3400 3194

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2025 Bryan Cave Leighton Paisner LLP.