Adoption of a Risk Based Approach to Inbound Payments

Background

Losses due to authorised push payment scams reached £583.2 million in 2021, an increase of 39% compared to the same period in 2020. UK Finance and its members believe additional measures and interventions are required to enable Payment Service Providers ('PSP') to prevent and respond to the scale of fraud encountered. The goal of risk based payment delays, both for sending and receiving PSPs, is to prevent consumers from becoming victims of frauds and to stop illicit funds reaching the criminals. UK Finance and its members are seeking the opportunity to intervene in more high risk payments permitting additional time to investigate.

This paper builds on our position paper on the role of the sending bank and the need for adoption of a risk based approach to enable intervention on higher risk payments. It highlights two further areas which need to be addressed to enable a holistic approach to facilitate the payments system operator and payment service providers to stop criminals benefiting from their crimes and ensure illicit funds are returned to victims: Adoption of a risk based approach for receiving PSPs and the need for adoption of an industry framework for funds repatriation.

Regulatory barriers to adoption of a risk based approach for receiving PSPs

PSPs are increasingly investing in complex inbound payment detection tools, actively identifying and freezing payments identified as higher risk of fraud as they are credited into accounts. However, this approach is not consistent across PSPs with some questioning the legality of the approach when considered through the lens of Regulation 89 PSR 2017. This is further enforced by FCA Guidance issued in November 2021 which states that the FCA recognise "*that in practice some processing of the payment by the payee's PSP may be needed before the customer can access the funds. The requirement for "immediate" availability, however, means that the time taken for this processing must be kept to a minimum and we see no reason why, in normal circumstances, this should be longer than two hours"*

PSP's terms and conditions enable the freezing of funds to address operational measures needed to ensure compliance with the Proceeds of Crime Act 2002 ('POCA 2002'). Payment Service Providers must credit funds immediately to a payee account upon receipt into the PSP account, under Regulation 89 of the Payment Service Regulations 2017 ('PSR 2017'). Regulation 63(5)(a) PSR 2017 expressly precludes PSPs from agreeing with consumers the ability to alter through terms and conditions the applicability of Regulation 89 which prescribes the payment processing timeframe. Accordingly, terms and conditions cannot provide a means to extend processing timeframes except where POCA is engaged, and funds are frozen. Given the limited time available following receipt of funds for PSPs to investigate and the lack of information within the payment message to enable identification and evaluation of concern, it is highly unlikely that receipt of a payment alone, will immediately result in grounds to formulate a level of suspicion to meet POCA requirements. Formulation of suspicion or reasonable grounds to suspect put the PSP under the obligations of POCA 2002 (to prohibit transfer of criminal property) which would then enable through application of terms and conditions, a PSP to freeze a customer's funds pending investigation. A number of checks that could be deployed cannot be mechanistically adopted e.g. through screening or monitoring and require elements of human decisioning thereby necessitating time to investigate.

Often receipt of funds may trigger an investigation and only post investigation will sufficient suspicion arise, by which point funds may already have been dissipated. Extending the time available to PSPs, from the payment being credited into the PSPs account to the availability of funds within the beneficiary account will enable a more thorough investigation and where suspicion is aroused, for a DAML to be raised. In such cases we would propose funds are not credited to the customer's account pending receipt of the outcome of the DAML. Engagement with the sending bank would be required during this period to validate whether the payment is considered fraudulent. Receipt of consent from the NCA would then enable repatriation, if determined to be appropriate, if a fraud had been confirmed.

Recommendations

We have explored providing guidance with the FCA and PSR but the timeframes for payment processing are expressly stipulated in PSR 2017 and so guidance cannot extend timeframes without being in direct contradiction to statutory provisions and therefore of no comfort to firms. Regulation 63(5)(a) expressly precludes the ability for PSPs to manage this risk through amendment to their terms and conditions. Accordingly, in the case of inbound payments, **we believe an amendment to Regulation 89 PSR 2017 is needed to provide firms with the ability in high-risk fraud scenarios to hold inbound payments and not immediately credit them to the payee's account.** We do not think a time period for crediting of payments should be provided for in these instances. We believe that this will drive consistency in interpretation and to further encourage the active implementation of inbound transaction monitoring tools, will support the effective implementation of Enhanced Fraud Data across the industry, and the subsequent freezing of funds.

We would also propose that this legislative amendment is accompanied by simple amendments to the FCA Guidance. Potential amendments are shown in red below as a starting position for consideration.

8.294 It is recognised that in practice some processing of the payment by the payee's PSP may be needed before the customer can access the funds. The requirement for "immediate" availability, however, means that the time taken for this processing must be kept to a minimum and we see no reason why, in normal circumstances, this should be longer than two hours, with the exception of higher risk payments. Where a payment appears to be higher risk, for example the payment is at risk of being a fraud, the payment may be delayed. The delay may be used to conduct additional checks, and where relevant and permitted within POCA contact the customer. PSPs must document the factors considered in their risk assessments and be able to demonstrate their justification for their overall risk based approach. It is also necessary for PSPs to be able to evidence that their overall approach is necessary to address the risk and to measure the outcomes from payments that are delayed.

For the avoidance of doubt, unless the payment concerned is received out of business hours or is identified as higher risk "immediate" can never mean the next business day. The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011 Chapter 8 (and whether the payment is received outside of business hours must be considered in accordance with paragraphs 8.290 – 8.292).

The need for a regulatory framework that supports fraud reimbursement

This paper details the current regulatory landscape; however, it is important to acknowledge the potential changes to Regulation 90 PSR 2017 proposed within the Financial Services and Markets

Bill[1]. If passed, this change will pave the way for a mandatory reimbursement model for APP Scams. This will ease a number of concerns but will not resolve the wider issues around customer mandate, civil liability and repatriation which are outlined in further detail in this paper.

Regulation 76 PSR 2017[2] provides clear direction that the payment service provider is liable for reimbursement in all cases of unauthorised fraud. The only exemption to this requirement is where the PSP has reasonable grounds to believe that the claim is first party fraud. Additionally, if the payer gives incorrect payee details, Regulation 90(2)(a) PSR 2017[3] imposes an obligation on the PSP to use reasonable efforts to recover the funds.

Where, however, a customer gives an instruction to transfer funds to a specified account and the payment is subsequently identified as being an authorised push payment fraud, PSR 2017 does not prescribe that the payment service provider is liable for reimbursement, neither is there an obligation on the PSPs involved in the execution of the payment to make reasonable efforts to recover the associated funds.

What progress has been made to date?

In 2018, recognising the increasing risk of APP and cognisant of the lack of consistency when responding to consumer claims, industry lead by UK Finance, developed and implemented the Authorised Push Payment Best Practice Standards ('APP BPS'). The APP BPS is a voluntary set of standards for Sending and Receiving PSPs to follow when processing a claim of an APP scam. The intention was that the development of these voluntary standards would improve the experience for customers by producing a more consistent information flow between PSPs, drive increased opportunities for beneficiary PSPs to freeze and repatriate funds, and drive faster response times for customers on scam claims.

An industry led working group with legal representatives considered the proposed activity of freezing and repatriating funds from the receiving PSP back to the victim PSP for the reimbursement of victims and concluded that it was not clear that this could be supported within the current legal and regulatory landscape, for the reasons outlined below. Nevertheless, for the benefit of the consumer, those PSPs participating in the APP BPS have been carrying out this activity at risk ever since.

What are the current barriers?

i. Breach of Mandate

Within PSR 2017 there is no direct mandate for PSPs to return funds to victims of authorised fraud. On this basis, where a victim (A) moves funds into an account held by a criminal (B) as part of a scam, should the beneficiary PSP choose to repatriate funds back to the sending account holder, it risks a challenge by B that the PSP has breached its mandate to B. B could in fact bring an unauthorised transaction claim against the PSP under Regulation 76 PSR 2017. So, by refunding the funds, the PSP is exposing itself to litigation risk that it would not generate if it did nothing.

[1] Financial Service and Markets Bill https://publications.parliament.uk/pa/bills/cbill/58-03/0146/220146.pdf

[2] Regulation 76 PSR 2017 https://www.legislation.gov.uk/uksi/2017/752/regulation/76/made

[3] Regulation 90(2)(a) PSR 2017 https://www.legislation.gov.uk/uksi/2017/752/regulation/90/made

The risk is magnified where A and B hold their accounts at different PSPs. In that scenario, B's PSP is exposing itself to risk to assist the customer of another PSP. In an unauthorised fraud scenario, B's PSP would only do so on the receipt of an indemnity from A's PSP. However, in an authorised scenario, as A's PSP has no liability to reimburse A within current legislation, an indemnity is not a suitable construct.

Many PSP include a term in the account conditions, to permit them to return misdirected payments. The difficulty here is that it is not easy to set timeframes for fraud investigations, so it would be problematic to set out rigid timeframes within terms and conditions. There is also the risk that this approach could be challenged as being unfair as per the unfair terms' requirements in the Consumer Rights Act 2015.

As a result, in the absence of legislation requiring the refund to be made, the current status quo will remain, resulting in inconsistency for the victim. The current landscape sees some PSPs accepting the risk that if the account holder B is not a fraudster, the PSP will be liable for the funds, but they do so to provide the best outcome to victims. Other PSP will not consider the repatriation of funds until evidence of a law enforcement crime report is provided, or consent is provided by the NCA.

ii. Compliance with the Proceeds of Crime Act 2002 ('POCA 2002')

Where the PSP has reasonable grounds for suspecting that the funds are proceeds of fraud, and therefore criminal property, the PSP will risk committing an offence under POCA 2002 if it repatriates funds without first gaining authorisation to do so from the NCA.

Where the funds sit within a first generation mule account, this process was made significantly easier in November 2019 when the NCA issued a new Glossary Code XXVICTXX and published guidance to reporters to help with the repatriation of funds to victims of crime. The guidance gives the reporter the option to either submit a SAR or DAML for this activity, where previously a DAML was the only option available. How the reporter chooses to report is left to their own discretion, but the introduction of this code meant that in cases where the receiving PSP can be confident that they are returning funds to the ultimate victim of a crime, they are no longer required to submit a DAML and wait for consent and can instead submit a SAR and complete the repatriation process.

Due to the complexities of establishing ownership for funds which are frozen in accounts at second, third, and subsequent generations, it is unlikely that the victim glossary code will be relevant and in almost all cases a DAML will need to be submitted and consent obtained. The process of obtaining consent will delay the refund to the victim, particularly if more than one PSP in the chain needs to seek consent. However, this does not remove the risk of a consumer raising a complaint for breach of mandate. Here, the application of POCA would seem to frustrate rather than promote the intended outcome and in so doing, creates a considerable operational demand on PSPs to manage as well as contributing to an unsustainable level of DAMLs for the UK FIU to manage.

iii. The risk of Tipping Off

The position becomes even more complex where there is a chain of accounts through which the money has passed, as in this situation the risk of tipping off increases. For example, in the following scenarios: B's PSP has frozen the funds in B's account and knows that A needs a refund but can also see a payment has come into the account from another person, H. B's PSP does not know whether H is another victim or potentially a complicit mule directing criminal proceeds to B. To understand whether funds should be returned to H, H and B's payment service providers would need to be able to communicate with each other about the circumstances of the possible fraud to enable clear identification of who is a fraudster and who is an innocent victim. B's PSP is aware of a further claim from customer J for which there are insufficient funds in the frozen account. In an

ideal scenario, B's PSP would wish to contact any subsequent PSPs who have accounts in receipt of funds from B to see if those accounts are held by mules and should be frozen and the funds returned.

In both cases, there is an exception from the general offence of tipping off under Section 333C POCA 2002 where the disclosure is made between PSPs for the purposes of preventing financial crime. This would allow the PSPs for A and B above to share information about the possible fraud. There is still a risk, however, that if the other PSPs contact their customers H or J to obtain further information about the case and to determine if they may be another victim, they may in fact be another mule and this could amount to tipping off. Contact with account holders must be handled with care the further away from the genuine victim the account sits within the transactional tree. There may be a defence if the PSP genuinely thinks that the customer is a victim as it may be able to argue that it did not know or suspect that disclosure was likely to prejudice an investigation. However, relying on this defence would be risky, particularly if the PSP has not conducted a thorough investigation before contacting the customer. It is not possible to get consent to tipping off, although in practice if a PSP obtained consent to contact their customer via a SAR the risk of any offence would be significantly reduced.

iv. Absence of an agreed methodology for allocating funds between customers

As well as the information sharing concerns, the allocation of funds between customers becomes increasingly complex where there is more than one victim identified. There is a risk that, in the absence of a strong legal framework and agreed industry approach, PSP's will react to claims from customers without knowing the full facts which will lead to a "first come, first served" approach to reimbursement. It also raises issues where there are competing claims received at the same time for only limited amounts. Where this happens, the "first come, first served" approach may not work as the first to come to the PSP may not have the strongest claim on the funds in the account.

In these cases, the relevant PSP may use the rule in **Clayton's case** as justification for applying funds based on the order in which they were paid – meaning the victims who had made the last payment into the account would potentially be in the strongest position. Again, this is risky for PSPs as there is no legal framework for the refund, which will itself be in breach of the customer's mandate, and this approach could conceivably be challenged by a victim who does not receive a fair share of the frozen funds.

In more recent years there have been precedents for funds to be distributed on a **Pari Passu basis.** The Pari Passu principle considers the problem of funds repatriation by dividing the pool of available funds proportionally between the victims, based on their proportion of total loss suffered. It does not consider the order of the transactions but only considers their relative amounts.

The allocation also potentially gives rise to the question of imposition of a **constructive trust**. Constructive trust is the relationship by which a person who has obtained title to property has an equitable duty to transfer it to another, to whom it rightfully belongs, on the basis that the acquisition or retention of it is wrongful and would unjustly enrich the person or PSP. Arguably, unless the beneficiary PSP can see only a limited number of payments going into the beneficiary account, as soon as it received the first claim, it may be on notice that the remaining funds may be the proceeds of fraud against not only that first victim, but numerous others, still to be identified. Whether a constructive trust will arise, will depend on the circumstances; the issue is whether the PSP is aware that there is a serious possibility that other victims, other than the first claimant have a proprietary right to the funds in the account. Depending on the circumstances there is a risk that the PSP could be held to be under a constructive trust to hold the funds for the benefit of all such victims. If the PSP paid out funds to the first victim, based on the rule in Clayton's case, it could still be challenged by other victims that the refund was made in breach of this constructive trust. This

would place a considerable burden on the PSP to investigate and ensure it had identified all victims before making any refunds. This is a serious concern for PSPs in the current landscape with APP scams becoming increasingly complex and with mule accounts more commonly being long standing accounts used for day to day payments where there may be the co-mingling of genuine and fraudulent funds which further exasperates the assessment of funds for repatriation.

v. How to define fraud

Finally, there is an issue of how the PSP would define fraud for these purposes. Where there is an unauthorised payment from the account, PSR 2017 effectively permit the PSP to assume the customer is telling the truth in the absence of evidence to the contrary. For authorised fraud, in the absence of that legal framework, PSPs need to be careful in how they set the boundaries and investigate any allegations of fraud. Although most claims are likely to be genuine, there is the risk that first party fraud may be occurring, or consumers are using PSPs as a reimbursement option for buyer's remorse. Note the high proportion of APP claims which fall under the category of purchase scams. Even now, three years after the implementation of the Contingent Reimbursement Code, there is no clear means for PSPs to distinguish between a purchase scam and a civil dispute.

Recommendations

1. 'First generation' repatriation where funds have been frozen and the sending PSP is able to confirm with certainty that the account holder is a genuine victim.

   BPS participating PSPs have taken a risk based approach to enable first generation repatriation. Outside of the BPS PSPs however, first generation repatriation is not always consistent. To encourage wider adoption of the BPS approach, we would suggest that the following steps are required to provide the necessary legal cover:

   - To remove the risk of consumers raising complaints for **breach of mandate**, amendments are required to the PSR 2017 requiring both sending and receiving PSPs to make reasonable efforts to recover funds where a fraudulent authorised push payment transaction has been confirmed, in line with the wording included within Regulation 90(2)(a) and 90(3) PSR 2017.

   - To address industry concerns around **civil liability,** which exists due to the potential for consumers to challenge based on the unfair terms clause in the Consumer Right Act, an industry agreed position with approved wording from HMT will be required for inclusion in PSPs' Terms and Conditions.

2. Reimbursement where funds have been dissipated through a chain of accounts, potentially with multiple transactional trees.

   - To drive consistency across PSPs, the industry legal working group should be tasked to agree an industry standard for funds allocation which demonstrates fairness to the victim(s), reliability of result and simplicity that is consistent across a range of APP claim scenarios.

   - Using modern technology, the industry should explore the options to trace backwards, confirmed fraudulent funds held in mule accounts, to identify the initial victim. As funds move further away from the victim, the certainty of ownership become less clear as there can be genuine accounts and genuine funds involved within the payment chain. In 2017, several PSPs working with a commercial vendor explored the potential in using complex algorithms to deliver this outcome. At the time, the findings from the proof of concept were poor with only a small percentage of traces leading to the ultimate victim. Five years on, the

same vendor holds significantly more data and has a far greater knowledge base, however the continued lack of legal framework to enable repatriation and conflicting priorities has led to the proof of concept not being re-established. To achieve the appropriate agreement on reprioritisation the vendor will need commitment that the necessary regulatory changes to enable repatriation are being considered by HMT and regulators.

Development of an effective process which can provide a high level of assurance that funds being returned are the property of the identified victim, will need to be established in parallel, with the proposed legislative framework.