This paper sets out the response to the questions raised. We and members believe it provides a clear evidence base to support the adoption of a Risk Based Approach (RBA) to payments. Indeed, the evidence would suggest that, in the absence of changes to regulations and legislation – where we would be happy to work with HMG and regulators to ensure the minimum impacts on legitimate payments – the type of fraud that we are seeing will only continue to increase. This will both see more money going to serious and organised crime (and possibly to destinations connected to hostile state actors) and reduce competition and growth in the UK. We are increasingly seeing that some members are taking a very risk adverse approach to business with all forms of crypto exchanges for example as the current legal and regulatory framework does not sufficiently support a calibrated approach based on risk. We have set out the evidence in response to the questions below:

- **Impacts on payments**: Paragraph 6 of the paper mentions that "*current modelling would suggest no more than a small percentage of payments being impacted*" and in paragraph 24 in relation to higher risk payments "*This profile varies across firms depending on type of customer and risk, but the view is these would commonly be less than 1-3% of all payments. We would see any impact on payments as being further below this range but is still being assessed*." - **are you able to share more on how you came to this assessment, including assumptions and data underpinning this?**

  When considering Faster Payments only, based on 2021 industry data 0.0098 percent of payments, or 1 in every 10,188 payments resulted in an Authorised Push Payment scam. When adding BACs and Chaps payments into the equation this value drops further to a total of 0.000035 percent or 1 in every 28,940 payments.

  When considering these statistics, we must recognise that not all scams are the same. The specific challenges faced by firms in detection and the lasting impact on victims will vary considerably across scam type.

  An analysis undertaken by seven of the Authorised Push Payment Contingent Reimbursement Model (APP CRM) firms, covering approximately 85 per cent of payment market share, in 2021 demonstrated that purchase scams formed the highest proportion of APP scam cases dealt with by Code Signatories. Set out below are the findings of the analysis highlighting APP fraud cases banded by value and reviewed as a percentage of the total APP cases across the APP CRM firms:

Purchase scams – Under £100	21% of all scams
Purchase scams – Between £100-200	15% of all scams
Purchase scams – Between £200-300	9% of all scams

  This demonstrates just under half of all APP scams across the seven APP CRM firms who participated in this data collation are purchase scams under the value of £300. Further analysis shows that 55% of all scams by volume are purchase scams, whilst by value, purchase scams account for just 15% of the total value of all APP scam claims raised. The low value, high volume nature of this scam type makes detection using traditional fraud control methods challenging, as a high proportion will fall within normal spending levels and patterns. Therefore, it is unlikely that ~~a~~ risk-based intervention

will be required. In the rare case that one is required, the time needed to engage the consumer and clarify the authenticity of the purchase, due to the relative simplicity of these cases, is unlikely to infringe on the timelines available within current regulation.

In contrast, whilst only 6% of all APP scams by volume are investment scams, they represent 22% of the total value. The high value, low volume nature of this scam type means that these are generally more likely to be detected by transaction monitoring tools, but pose a very different challenge for firms as, when detected, it can be difficult to deter customers from making what they believe is a sound investment using warnings alone. Romance scams too pose similar challenges. Amounting for only 2% of all APP scams by volume, but generally high on value per case, when detected, it can be both a time consuming and challenging task for firms to convince a consumer, who may have been in contact with the scammer for considerable time, that they are not in a relationship with that person and are instead the victim of a complex scam. In these cases, firms will need to employ a multi-layered engagement plan, often including the intervention of law enforcement, to 'break the spell', and the risk based intervention to be effective will frequently need to exceed the day-plus-one available to firms within current regulations.

The above therefore demonstrates that generally it is only the high value, low volume payments which occur in exceptionally low numbers which will require a risk based intervention exceeding day-plus-one. To fully illustrate this, it is worth considering that the total percentage of payments resulting in an investment or romance scam in 2021 was 0.0018 or 1 in every 228,227 payments. Therefore, for the average customer, the ability for firms to apply a risk based approach will not impact their payment journey, but when required, risk-based interventions will primarily be for the most vulnerable customers and where life-changing sums are involved.

That said, we would caution HMT not to set an industry threshold for the per cent of payments per year for which firms are authorised to apply a risk based intervention exceeding the current regulatory timeframes, based on these numbers. As and when industry solutions are introduced, there may be fluctuation. For example, the Enhanced Fraud Data initiative being developed by UK Finance and its members may initially highlight an increased number of payments which require intervention. Industry must be able to learn and adapt and to have the flexibility to respond to changing modus operandi (MOs).

It is important to caveat that UK Finance does not collate management information for prevented authorised push payments. The number of payments already prevented by industry is therefore not included in the figures above. It is also important to state that there will always be an element of false positives when employing fraud detection strategies. However, even with these caveats, current industry data indicate that across firms, alerts are only generated on between 0.04% and 0.2% of payments. If we were to assume that 10% of these alerts were to result in a risk-based intervention which may exceed the current regulatory accepted timelines, this would only apply to between 1 in 1,367,092 and 1 in 6,835,461 payments.

- **Impacts on fraud**: In paragraph 27 you note in relation to impacts on fraud "*The level of impact depends on the level of grit permitted based on further modelling to be done in conjunction with the public sector.*" **Do you have any existing analysis demonstrating the impact of length of delay**

versus fraud prevention, and if so, could you share this (including underlying data and assumptions)? Would this have benefits for all scam types, or some more than others?

In responding to HMT's request for further policy evidence, it is important to restate the position that tackling the APP scam epidemic requires a multi-layered approach. This includes responses at the point of payment, such as dynamic risk assessments, a risk-based approach to payment interventions, and wider industry and cross sector data sharing. The wider question for all key stakeholders is why the UK's payment system is so attractive to criminals and what, if anything, can be done to mitigate that.

On this wider point, UK Finance and its members believe that risk-based delays will help to lessen the UK's appeal to criminals. Recent comments from Chris Helmsley, CEO of the Payment Systems Regulator (PSR), in his Counter-Fraud Conference keynote speech, point to an appreciation that the very speed within the Faster Payments System (FPS) is perhaps contributing to the APP fraud problem.

"It seems to me that a payment to a friend should look and feel quite different from when I am using my account to buy something. And feel very different when I am moving life-changing sums when buying a house. This points to the need to create clearer distinctions between different types of payments; likely backed by new branding and trustmarks, so that customers understand more about the protections that they can expect."

We also note that Damian Hinds, Security Minister, has asked for evidence in the past to explore how international markets and their payment systems compare to the UK.

The UK's FPS system is market-leading in terms of the pace with which funds can be moved around the system. This will potentially become faster when the New Payments Architecture is delivered. The concept of risk-based payments is not just about how risk based payment delays to enable targeted interventions may prevent losses in individual payments. It is also about how we reduce the attractiveness of the UK as a target for fraud and fraudsters.

As outlined in our response to the previous question, not all scam types are equal and as such they require differing detection tools, strategies, and subsequent engagement methods to 'break the spell'. Data received from industry indicates that across firms, alerts are currently generated on between 0.04% and 0.2% of payments. Of these alerts, a high proportion will be resolved on the same day following review by a fraud agent: however, where concern remains, customer engagement will be initiated. As explained previously, the more complex scam types, such as Investment, Romance, and Impersonation scams, may require ~~a~~ more targeted risk-based intervention. The length of time required to ensure both parties, (i.e., the consumer and the sending Payment Service Provider), are comfortable with the authenticity of the payment, will depend on the individual case. The table below provides an indication of the resolution and time taken following a payment alert being generated, in this case by the sending Payment Service Provider (PSP). (N.B. these data are derived from one PSP who has taken the policy decision to exceed day-plus-one ('D+1') where concerns remain about the authenticity of a payment):

Table 1:

	Same day	D+1	D+2	>D+2

Confirmed Scam	92%	2%	2%	3%

This demonstrates that a significant volume of alerts are resolved on the same day, with a far smaller proportion on D+1. However, this data also demonstrates that up to 5% of scam alerts, are resolved after the D+1 cut-off. This is an indication of the benefit which may be derived from the provision of regulatory comfort / reform to enable consistency in interpretation and allow wider industry to hold payments past day-plus-one where concerns are present.

The case studies below demonstrate the impact a more tailored and complex intervention can have on firms' ability to break the spell and protect consumers. The firms involved in these cases took this approach at risk, and this is not reflective of the standard industry response, but is demonstrative of the approach we would expect to see if legislative change where to be agreed

Case study one:

Mrs M (82) became known to Customer Care when she contacted the bank to authorise a faster payment for £475,000. Through discussion with the customer, it was clear that she was involved in a romance scam. Her good friend was unable to secure a mortgage and was renting, so she wanted to gift him the funds to allow him to buy a property. Her friend (62) had confirmed he would amend his will so that should he pass before her, he would gift her the money back on his death. When the bank declined the request, the customer looked at various other options, one being to apply for a mortgage in joint names. We were concerned the customer was being financially taken advantage of and had numerous conversations with her. Despite our best efforts, the customer would not accept that this was anything more than helping her friend, and continually called suggesting new ways of how to send the funds. The customer then advised that she would purchase the house outright herself and draw up a joint tenants' agreement with him; she would not live there, but he would. As each request was declined, it became increasingly concerning that the customer was being pressurised to call to discuss with us how she would be able to transfer the funds. When we advised we would not send any funds to her friend directly or indirectly through a solicitor or third party, our customer requested the funds be returned to the investment bank from which she had sent them and advised that she would send the funds from there instead. We contacted the investment bank regarding our concerns, and they confirmed that a similar request had been made by Mrs M to send this amount to her friend. They also advised Mrs M that they would not send any funds to the named beneficiary.

After a case discussion and persistent ongoing attempts from Mrs M to affect the transfer of funds, Banking Protocol Cross Channel (see Annex A) was invoked. Police attended Mrs M's home address to discuss with her the current situation and their concerns for her financial welfare. Mrs M's family was contacted, and with further support from family members, they were able to convince her that this was a scam and to break all ties with her friend.

The bank has since agreed to transfer the funds back to the investment bank to allow Mrs M to continue to receive a return on her savings. Customer Care continues to monitor the account and offer support to Mrs M on an ongoing basis.

Case study two:

A customer transaction flagged as suspicious when trying to create a new payee and issue a payment on the bank's online platform. The customer's bank made an outbound call to the customer to ask for additional information. The customer advised that the payment was for an investment and that whilst they acknowledged the bank's concern they still wanted to proceed. The bank asked additional questions and, not being fully comfortable with the answers provided, asked the customer to attend their local branch to supply additional verification for the payment. The customer refused and at this point the bank informed the customer that if they wanted to proceed, but were not willing to attend a branch, the firm would issue a referral to local law enforcement and ask that they arrange to visit the customer at their home.

When police attended, the customer was hostile towards the responding officer, however the officer was able to obtain enough information to be confident that the investment was a scam. The customer still wished to proceed with the payment; however, the customer's wife (who had not been aware of the proposed investment) asked that the officer return the next day when their son was due to visit. The attending officer kept the bank informed of progress throughout.

Following the officer's second visit, the customer recognised the risk, contacted his bank, and thanked them for going 'over and above' in their effort to protect his savings.

The following case study demonstrates where a payment delay or more complex intervention may have helped to break the spell, but where the firm did not believe that they had the flexibility to take any further action.

Case study three:

This case study concerns an investment scam totalling £262,000. The customer (76) had been with their bank for 56 years. She was seeking investment opportunities, and had located an advert in a newspaper, outlining how to make money from bitcoin. The customer filled in her details and was then contacted by an investment firm.

The customer subsequently acted on the scammer's instruction on how to invest, opening the relevant bitcoin accounts using genuine details, transferring funds into the wallet, and then using the wallet to move funds to the investment firm's wallet. The customer did not heed any warnings provided by the bank and continued to make payments even after Banking Protocol was used and police attended the bank branch.

Multiple blocks were applied to the account, but the customer always visited the branch to have these removed and confirm the payments as genuine. Whilst concerns remained, the bank did not believe they were able to hold the customer's funds indefinitely or delay a payment further given the legal framework.

When communication with the scammer stopped, the customer finally realised she had been scammed.

- **Evidence on how payment service providers currently delay suspicious payments**: we note that several major banks already do delay suspicious payments, and explicitly state in their Terms and Conditions that they may do so; we'd be keen to understand where possible:

- the volumes and values of payments that are delayed, including how long these payments are delayed (how many/ what proportion are delayed within D+1, how many/ what proportion are delayed beyond D+1)?
- What volume/ value/ proportion of payments that are subsequently found to be fraudulent do banks currently detect, delay, and prevent?

As previously outlined, data received from industry indicates that across firms, alerts are currently generated on between 0.04% and 0.2% of payments, the equivalent of between 1 in 136,709, to 1 in 6,835,461 of payments made. Where an alert is generated, the payment will be held to enable the risk to be assessed in more detail. Of these alerts, a high proportion will be resolved on the same day, following a review by a fraud agent. However, where concern remains, customer engagement will be initiated.

Firms have varying customer engagement strategies, using a combination of voice calls, in-app messages, and SMS self-service. Where concerns remain and PSPs are unable to break the spell, they may invoke either the in-branch or remote version of the Banking Protocol. Where the PSP is not able to contact the customer to verify the transaction, firms will generally hold the payment and reverse the transaction at a set date and time. The length of time for which a PSP will hold the payment will depend on their interpretation of the current Payment Services Regulations (PSRs). Where the PSP has made a policy decision to enable payments to be held past day-plus-one, the length of time required to ensure both parties, (i.e., the consumer and the sending PSP), are comfortable with the authenticity of the payment, will depend on the individual case. Figure 1 demonstrates the average length of time taken by one PSP to reach a point of agreement between both customer and sending PSP regarding the authenticity of the payment. As mentioned previously, this data demonstrates a volume of payment alerts which exceed the D+1 available within the current PSRs and therefore the significant benefit which may be derived in providing regulatory comfort / reform to deliver consistency in interpretation and enable wider industry to hold payments past day plus one where concerns are present.

Data obtained from one PSP who does not allow payments to be held past day-plus-one is equally insightful. This data indicates that whilst 62 per cent of alerts are resolved within day-plus-one, 38 per cent are reversed having reached the day-plus-one threshold without resolution. Of the 38 per cent, 8 per cent are resubmitted for payment by the customer and will be subject to the same fraud risk profiling, whilst a significant 30 per cent remain unresolved. In the case of the 30%, the PSP is unsighted on the consumer's decision-making. The consumer may have chosen not to proceed with the payment having had time to consider the payment reason, alternatively, they may have proceeded via an alternative payment provider or method with potentially lower fraud controls in place. There is a question therefore, if the policy decision to cancel payments at D+1 places consumers at a higher risk of subsequent financial harm, compared to the alternative of delaying the payment further to enable the PSP to continue engagement through to resolution. It also demonstrates the need for the industry to have stronger consistency across approach on payments (as above there is a great deal of variation in the approach firms take to delaying payments, which will be based on legal advice and risk appetite) and more easily share information on 'at risk' customers.

Further legal analysis

- **Evidence** on **how payment service providers understand the existing framework to delay suspicious payments**: we'd be keen to understand further how the individual PSPs that currently delay payments beyond D+1 understand their legal position in relation to delaying payments, how they make decisions to do so, and what evidence they require to proceed with a payment after investigation, including noting if views differ amongst members.

  As the UK Finance paper indicates, the legal grounds for firms to delay payments beyond D+1 are currently narrow, limited to where POCA or the Quincecare duty applies (noting the latter is now less certain due to the ongoing Barclays ss Philipp case). This means that setting wider parameters for payment delays involves firms balancing the risks of customers falling victim to fraud and the firm's liability to refund, against the risks of being challenged around breach of mandate and legal compliance.

  Of the firms who provided UK Finance with data to support this response, the majority had made the policy decision not to allow payments to be held past the current day-plus-one threshold. The only exception was where Banking Protocol Cross Channel was invoked, and law enforcement engaged, however, this exception is not consistent across all firms.

  The PSPs who do delay payments past D+1 on the whole believe that they are doing so at legal risk. Given the public policy importance of fraud that seems a palatable position. The PSRs contain general requirements to meet the D+1 timeframe. They do not include anything specific on delaying payments, but do set out at Regulation 71, grounds under which a payment instrument can be stopped generally; and at Regulation 82, requirements around the refusal of payments, with 82(5) indicating that firms can include terms in their conditions allowing for such refusal. Contractual terms permitting payment refusal are however subject, for consumer payments, to unfair terms' requirements in the Consumer Rights Act and, generally, to challenge that the firm is acting in breach of its customer mandate to execute payments, particularly where such terms are more widely drafted, giving significant discretion around refusal.

  Where firms currently impose delays due to concerns of fraud or other financial crime, and include contractual terms allowing such delays, they are generally taking a risk-based view. Given the push, rightly, from regulators and HMG for the industry to do more to prevent fraud, it seems perverse not to provide the industry with the regulatory comfort to support a stronger risk based approach. As outlined in an earlier question response, the negative impact for the consumer of an extended risk-based payment delay will often be less than a full payment refusal. Additionally, the delay enables an extended period for the PSP and consumer to reach a point were both parties agree on the authenticity of the payment. It does, however, require risk acceptance, because there is always the risk of a consumer complaint, particularly in cases involving investments or where a payment delay may have impacted the consumer's ability to accrue interest on the account.

  UK Finance and its members strongly believe that there is benefit in amending the PSRs to enable delays where there is a suggestion of enhanced fraud and financial crime risk, due to the significant proportion of firms who have taken the policy decision not to delay past D+1 due to their interpretation of current legislation, the inherent risk of unknown outcomes due to the lack of visibility of the consumer's decisioning following the reversal of payments, combined with the significant level of risk acceptance required for firms to hold payments based on the current regulatory framework

- **POCA –** for further reference, while noting we are not currently exploring POCA as a legal avenue for delaying payments, we would appreciate if you could share any more detail behind your legal assessment that POCA is not an appropriate mechanism where possible, including any evidence form discussions in 2018.

  We believe that this has now been addressed and a comprehensive answer already provided to HMG where there is agreement this is not a suitable vehicle, legally or operationally. As such we have not expanded further.

Prioritisation

- **The relative value and priority of these proposals in relation to other existing and proposed measures:** (e.g., roll-out of Confirmation of Payee) and other proposed measures (e.g., enhanced data sharing as per PSR Consultation). While noting that fraud prevention measures can be complimentary, we'd like to discuss the priority of these proposals in relation to other measures underway in terms of fraud prevention, and where progress on fraud prevention can best be unlocked.

  UK Finance and its members see the delivery of a clear legislative framework, providing firms with the comfort to intervene where they perceive genuine risk and not to be limited by relatively constrictive timescales, as fundamental to the success of future industry measures such as the Enhanced Fraud Data Initiative. However, we also stress that the delivery of payment delays must not be achieved at the expense of enhanced data sharing. It is critical that these measures both be delivered in a timely manner.

  The data shared in this response clearly shows that investment scams make up a low volume of payments but a high value of losses. Industry data also indicate that two thirds of investment scams go unreported by consumers for 30+ days, until the consumer fails to receive their first monthly return.

  If we prioritised a standalone payment delay approach at the expense of the enhanced data sharing initiative, we may miss opportunities to identify payment risk due to lack of insight. If the sending bank were to identify a payment as high risk via existing fraud profiling tools, they may record the payment as an investment and potentially delay for D+1 to discuss the payment with the customer. However, delivering the enhanced fraud data initiative will mean the receiving bank can also be notified that the payment reason was an investment, alongside the sharing of enhanced fraud data relating to the sending customer giving them the opportunity also to assess the payment reason versus their account holder's profile, providing two opportunities to prevent and protect

  Where a risk is identified by either firm through the enhanced data shared, the ability to delay sending the payment or for the receiving firm to hold on to the payment upon acceptance may assist in preventing a scam on day 1-3 rather than reacting to a reported fraud on day 30, as is currently common today.

Annex A: Background on Banking Protocol

The Banking Protocol was developed in 2016 in response to the increasing risk posed by authorised push payment scams. Under the Banking Protocol scheme, branch staff are trained to identify risk indicators which may suggest that the customer is being scammed and, where necessary, to make an emergency call to Police.

Since its inception, the initiative has prevented more than £200 million in financial losses. Cases range from rogue traders who demand cash for unnecessary work on people's property, to courier scam fraudsters who persuade their victims take out a large sum of cash and hand it to someone posing as a courier.

Recognising the success of the initiative, industry has continued to work with law enforcement, expanding the scheme to telephone and online banking channels, known as Banking Protocol Cross Channel (BPCC). The expanded initiative ensures a police response to the homes of vulnerable victims who have attempted to make a payment via online or telephone banking channels, which were then flagged as potentially being part of a scam.

Where transactions flag as suspicious and the PSP is unable to break the spell, customers are asked by the bank to visit their local branch to complete the transaction, enabling branch staff to carry out additional checks and use the Banking Protocol police response if necessary. However, if the customer is unable to visit their bank branch, for example if they are vulnerable or have a disability, staff are now able to alert the local police directly, who will make a visit to the customer's home and assess whether they have fallen victim to a scam. Until the police response is received, the customers payment is held.

Early indications suggest this new approach is already proving successful, with one referral alone preventing the loss of £165,000 to a romance fraudster after the transaction was reported to police by telephone banking staff as a potential scam.

However, to gain law enforcement support for this initiative a Service Level Agreement (SLA) of 72 hours had to be built into the process from the point of the first referral to the responding officer to the point of the officer reporting back to the referring firm. Whilst the majority of BPCC referrals are completed within this time, some firms have been resistant to use the process due to the risks of going outside of the timeline allowed within PSR 17.

The Faster Payments System and Fraud

Summary

1. The paper below, and the accompanying Annex A: the Payments Journey sets out industry thoughts on how the speed of the Faster Payments System (FPS) can be exploited by fraudsters and proposes why and where changes are need to the legislative and regulatory framework.

2. The FPS undoubtedly offers tremendous benefits to legitimate customers and businesses in terms of speed and certainty of payments. However, those features are also exploited by fraudsters to get victims, often under emotional duress, to make a near instantaneous payment, and then disperse funds and cash out proceeds before the victim or the financial sector can act.

3. Currently payments must be treated the same – within a narrow timeframe – irrespective of fraud risk in behaviour or destination. The current regulations do not allow payments to be held for greater than 1 day, even where a bank believes the customer is being scammed and contact attempts are being made. We believe changes to the Payment Services Regulations 17 (PSR 17) could allow sending firms greater flexibility to adopt a risk-based approach to pause and investigate higher risk. This would allow further investigation and/or contact of the customer and more closely align the ability to intervene on suspected fraud payments with money laundering.

4. Firms assess risk by judging a range of factors including the profile of the account they hold, assessing the criteria of payments sent and received by that account, and if the sending and/or destination account has other additional risk factors. If there are concerns that the funds are possibly criminal or that the recipient is otherwise designated by HMG as not able to receive funds – such as on terrorist financing or sanctions, there is a range of legal tools to intervene.

5. However, we do not believe those same powers apply where the sender is not 'suspect' and the payment is 'clean' – even if funds are transferred because of deception. This creates challenges, especially given the methodology fraudsters use, of using warnings to break the spell on a victim. Once the victim has transferred funds, interventions are increasingly ineffective. This means gaps in the powers on fraud impact the ability of firms to manage the risk.

6. We do not envisage this causing delay to the majority of payments – current modelling would suggest no more than a small percentage of payments being impacted – and many of those would still be made within 1 working day. We also suggest means to mitigate impacts on legitimate payments. However, developing such an approach with the support of regulators and law enforcement could be calibrated to have a disproportionate impact to help cut impersonation and investment scams. We also believe this aligns with the proposals by the Payments Services Regulator (PSR) on risk scoring payments.

7. In terms of next steps, we would like to:

- get a definitive position on the current legal position to slow or delay payments.
- work with regulators, HMG, and law enforcement to draw up options and more detailed methodologies depending on different risk factors to support more detailed modelling on impact.
- discuss, with regulatory comfort, allowing some firms to pilot such an approach for a small discrete type of higher risk payments ahead of any legal change.

Fraud: a UK Problem

8. Fraud is a growing problem globally[1] but members with a global footprint view banking fraud as more significant in the UK than any other jurisdiction and consistently report that the % of scams they see in the UK is significantly higher than their % of UK bank accounts. This ranges from an average minimum of 15-40% depending on size and type of business model.[2]

9. Industry analysis of the factors behind this is at Annex B. Whilst there are several factors, including that English is the world's second language and the extent of online integration, a key factor is the speed of payments. The UK Faster Payments System (FPS) is world leading and payments move faster than almost anywhere. However, this same speed and certainty is also exploited by fraudsters. There has been a significant growth in scams in Australia (a rise of over $220 million in one year alone[3]) that tracks closely with the wider roll out of the Australian FPS.

Why is speed so important?

10. The FPS allows payments for up to £250k (rising to £1 million on February 8th) [4]and makes them routinely in less than a second, normally within 15 minutes, and over 98% of eligible payments are made within the industry tolerance of 2 hours[5] exceeding the requirement of 95% within 2 hours. Given the volume and pace scam payment are not easy to spot - the proportion of scams in 2020 was less than 0.068% of all faster payments.

11. Confirmation of Payee (COP) provides a layer of protection[6] but fraudsters have adapted and many APP Code signatories now see around 50% of scam payments go initially to firms outside CoP signatories. Once the payment is made, the chances of recovering funds increasingly diminish. Mules Insight Tactical Solutions (MITS)[7] shows fraud proceeds will commonly[8] start to be moved on within a timeframe of several minutes to two hours, sometimes through the use of bots to start to split and move the stolen funds to keep it below industry detection thresholds.

12. Industry data suggests over 99% of frauds are reported a significant period after the scam occurred, so funds are often moved and dispersed before the scam is reported. For example, one large UK retail bank in 2021 saw the following reporting timeframes (which are fairly typical)[9]:

Fraud Category	**Average days to report fraud**
Investment Scam	53.40
Impersonation Scam - Police / Bank Staff	5.64
Impersonation Scam - Other	7.72
Average (Combined)	**20.31**

13. Where funds are repatriated it will normally be because the 1st generation mule, often unwitting, has not moved the payment on fast enough and/or the receiving firm has 'frozen' the funds pending further investigation (again the legal position on this is not clear so not all firms do this). In short, wating for post scam reporting means the opportunity to intervene is sub optimal. The answer is increasing prevention (through expanding and making the risk perimeter more effective) and disruption – both at initial payment and tackling cashing out. To do this the banking sector needs powers to more easily pause payments and/or release of funds where a risk of fraud.

Legal Position

[1] The PWC Economic Crime Survey 2020
[2] This assessment was produced for Q3 2021. Figures are being updated to reflect 2021.
[3] https://www.auspaynet.com.au/sites/default/files/2021-08/Fraud_Report_2021.pdf
[4] It will be for individual firms to decide whether to apply the £1million limit
[5] The exceptions being due to system outage or due to targeted industry intervention
[6] At January 31 2022 CoP covered 31 firms and 95% of payments)
[7] Which covers 16 participating banks and nearly 95% of the market share.
[8] Currently estimated as over 65% and timings vary dependent on the stage in the mule network
[9] We excluded Advance Purchase scams, as they may not be suitable for delay, but they will normally several days after .

14. The Payment Services Regulations 2017 (PSRs 17) are clear on the need to make and release payments within 1 business day[10] and regulatory and customer expectation has been 15 minutes. The PSRs 17 and case law on the 'customer mandate' (Tournier) means there is no obvious means for sending firms to slow payments further. Our rationale for why POCA is not suitable legally or operationally, (despite recent suggestions this is a possibility is at Annex C).

15. We have a similar situation for receiving firms. Many firms have implemented inbound transactional monitoring and are actively, successfully freezing funds as they are received. However, this approach is inconsistent, and some firms question the legality of the process when considered against the requirements within Regulation 89 of the PSRs 2017. Where receiving firms do identify and hold funds, we ask for regulatory comfort and protections to allow firms to assess, on the balance of probabilities, claims of fraud by a customer and seek return of any of the customer's funds that have been able to be frozen, alongside protections for the receiving PSP to freeze and release funds back to the sending firm following an assessment of fraud.

16. Conversely, elsewhere the need to pause payments for longer than 24 hours is accepted. There are already strong legal protections in place – including POCA – for firms to delay and investigate payments, and even to seek 'consent' where there is concern of money laundering, sanctions evasion or terrorist financing. The ability to slow payments where funds are otherwise clean, but there is a concern around fraud risk is out of kilter with those on money laundering.

Why it matters

17. The Lending Standards Board (LSB) has found that firms need to develop more effective warnings to 'break the spell' of fraudsters on a customer. This can be difficult within a 24hr timeframe, particularly when customers will often fail to respond to calls or e-mails from their bank within 24 hours (and a tool of fraudsters is to create distrust of official bank communications).

18. Equally some firms will not sign up to the extension of the Banking Protocol (more detail at Annex D) to cover telephone and internet banking as police forces have said they cannot agree a Service Level Agreement shorter than 72 hours to contact a customer where a risk of fraud in these payment channels. As this is outside the legal framework for delaying payments, many firms – who are otherwise signatories to the in-branch BP - see no point in signing up.

19. Finally, firms respond to the legal framework and regulatory expectations they operate within. The system is currently calibrated towards speed and firms are left trying to graft on limited friction, often with little impact. There has not been a strong consistent steer to support higher risk payments being slowed down to investigate further. Changing that will require a strong signal from HMT and the PSR, not least many customer complaints relate to delays in payments.

Introducing the necessary flexibility to manage risk

20. Currently all payments are treated, within a narrow timeframe, as similar in terms of risk. In the same way, all destinations are treated, legally, as posing similar fraud risk - even though neither is true. Being able to adopt a risk-based approach, depending on risk factors individual firms see, to more easily delay sending payments and/or releasing funds for a short reasonable period (at times beyond 1 working day) would help reduce fraud and protect customers.

21. This would align with an increasingly customer centric view of risk firms are introducing. It supports PSR proposals on risk scoring payment messages and could support onward investigation where a higher risk of fraud. For example, a sending firm scoring a payment as higher risk could delay the payment pending further investigation and/or inform the receiving firm

[10] (Regs 86-89)

who could also decide whether to investigate the funds until concerns are resolved. This would help reduce repeat use of mule accounts and maximise the potential of technology.

22. However, for any future data sharing solution to be successful, it will need as above, amendments to the PSR 2017, or, at a minimum, regulatory comfort given the PSRs 2017 mandate payment execution timescales. Whilst firms can intervene, warn, and advise customers where it is believed they may be being scammed, firms currently have no regulatory comfort to stop the execution of that payment unless instructed by the customer to do so. The ability to better share data also needs to be accompanied by the ability to better intervene.

The level of delay – how much is right?

23. That is to be determined – through work with HMG and regulators – to reach a view on the collective risk tolerance. However, we envisage this being used relatively sparingly on a risk-based approach based on both individual firm and collective intelligence assessments (such as where some PSP and/or crypto exchanges are increasingly source destinations for fraud losses).

24. The level of overall scams, relative to total payments is less than 0.07%. However, certain risk factors are more prevalent with scams and rise when in combination. For example, a common higher-risk scenario would be (a) a payment for all or nearly all or a high % of the customers funds or savings; and (b) the recipient is for a firm outside of the CoP; and (c) a receiving destination that is increasingly associated with higher subsequent rates of fraud reporting based on individual firm and industry intelligence. This profile varies across firms depending on type of customer and risk but the view is these would commonly be less than 1-3% of all payments. We would see any impact on payments as being further below this range but is still being assessed.

Impacts on payments and on customers

25. We want further discussion on methodology and risk tolerance with HMG and regulators but at present would envisage a risk-based approach impacting no more than a small percentage of payments or release of funds in total. Even then, many of these may still be made within 1 working day depending on further checks and contact with the customers. This working figure reflects that new payees account for approx. 10% of all payments (all routinely receiving a warning). Within that only a small proportion are subsequently reported as scams of which over half are advance purchase scams – which will tend (though not always) for smaller amounts and where a delay – beyond that already available - may not be appropriate.

26. Introducing the ability to delay release of higher risk payments would provide more customers with greater protections from fraud. However, we accept some genuine customers would be impacted. Therefore, in introducing such an approach, members would need to have the ability to lift any delay so e.g., if a customer was being adversely impacted by a 48-hour delay, they could contact their bank to request the payment is made more quickly. This would also provide greater opportunity to ‘break the spell’ if the customer was under duress from fraudsters.

Impact on fraud

27. The level of impact depends on the level of grit permitted based on further modelling to be done in conjunction with the public sector. Equally fraudsters would adapt and so risk scoring would in turn need to calibrate. But an initial industry view is that, if properly scoped a targeted focus on higher risk payments would have a disproportionate impact on fraud and could help reduce the volume of investment scams and impersonation scams.

How to do this

28. We believe changes to the PSR 17 to bring the principles and protections on fraud for sending firms in line with money laundering would be needed. We have set out one means by which this could be achieved at Annex D – although this is only a starter for discussion. As an interim, we believe the use of regulatory statements could help provide regulatory comfort for sending firms.

Annex B: Drivers of Fraud

29. Figures vary as each firm has a different business model but for example:
    - A large UK retail bank, with a significant global presence, sees nearly 70% of all their global fraud occur in the UK.
    - Another retail bank has less than 25% of accounts in the UK but over half all their fraud is in the UK.
    - One FinTech with a large global presence has 15% of their accounts in the UK, but over 65% of all scams they see happen in the UK[11].

30. Industry analysis suggests several factors in combination drive the scale of fraud in the UK:

- **English language** – as English is the world's most popular second language this means fraudsters operating overseas can easily target the U.K.

- **Extent of online and mobile banking and decline of cash –** online banking by UK citizens compared to the EU, US and Australia is particularly high and the public and private sector is increasingly **digital by default** – for example online shopping is far higher than the EU average.

- **Faster Payments System –** the UK Faster Payments System (FPS) is world leading and payments move faster than almost anywhere. However, this same speed and certainty is also exploited by fraudsters. There has been a significant growth in scams in Australia (a rise of over $220 million in one year alone[12]) that tracks closely with the wider roll out of the Australian FPS.

- **Ease of cashing out** – the use of multiple accounts by individuals is higher in the UK than comparable countries, KYC is more flexible than most EU counterparts and there is no single identifier per resident. We have limited restrictions or currency reporting on international banking (unlike Australia); and a higher volume of MSBs than comparable jurisdictions.

The Industry Response

The sector spends over £1.5 billion a year to tackle fraud with some success, preventing £736 million in unauthorised fraud in the first half of 2021 - equivalent to £6.49 in every £10 of attempted unauthorised fraud being stopped. However, many of the defences on unauthorised fraud are built around verification of the customer. On authorised fraud, the same defences do not work – as it is the customer authorising the payment, checks on the customer are bypassed

Annex C – the use of the Proceeds of Crime Act to slow/delay payments

<u>Legal Position</u>

PSR 17 and regulatory interpretation

- The PSR 17 sets out the requirements by which the speed of payments must be made. We see no other powers or tools, in the absence of regulatory statements to the contrary that would safely allow firms to slow down payments outside of the timescales mandated in the PSR 17 in relation to payments being made by a possible victim of fraud. Indeed, the regulatory

[11] These figures are historical and industry figures are being updated to reflect 2021
[12] https://www.auspaynet.com.au/sites/default/files/2021-08/Fraud_Report_2021.pdf

expectations have traditionally been payments should be made far faster than the PSR 17 timeframes.

- Regulatory statements would be an option to provide clarity on interpretation – it is HMT legislation and therefore perfectly proper for HMG/regulators to provide supplementary advice on interpretation. We have previously suggested ahead of legal change regulators could provide good faith protections to allow firms to slow down payments (even if outside of PSR 17 timescales) for a short period to allow them to investigate where there are reasonable grounds to believe the payment may be fraudulent. However that has not yet been forthcoming.

POCA as a basis for slowing down payments

- The industry view is that it is difficult to see how POCA would bite as these are not yet the proceeds of crime – this would be similar to ransom payments where it is not illegal per se to pay a ransom and the ransom does not become criminal property until it is in the hands of [the] criminals.

- This position is supported by the Supreme Court Case (R v GH) which confirmed that money only becomes criminal property when it is in the hands of the criminal by reason of the fraud perpetrated on a victim (https://www.supremecourt.uk/cases/docs/uksc-2014-0035-judgment.pdf.)

- Even if a Defence Against Money Laundering (DAML) SAR was submitted it would again be difficult to see under what basis the NCA could grant or refuse consent, again as it is not yet criminal property. We are not aware, outside of Terrorist Financing and Sanctions, any legislation or regulations where funds can be blocked on the mere possibility they may become illicit finance in the future. Even then these powers relay on designation on recipient as opposed to the funds themselves.

- This issue was considered in 2018, ahead of the publication of the APP Code, by a joint legal working group comprising, amongst others, industry lawyers, the Home Office, HMT, the PSR and the FCA and POCA was not seen as a suitable tool for delaying payments.

If POCA were to be used to slow payments

- If it were decided POCA was a suitable vehicle - and guidance/statement would be needed to make that explicit - then the operational consequences to payments and for the NCA would be significant and would require a lot further thought as the logical consequence of such a position would be that a firm had to submit a DAML SAR in order to engage the POCA framework (and in turn the defence for not following the customer mandate).

- For example, if the NCA were to decide they could opine on whether to proceed or not, it would lead to a significant uplift in DAML reports being made and the NCA asked to give a view and would make the NCA the de-facto assessor of if a payment was fraudulent or not. If they decided to grant, then there would be no legal impediment to proceeding, which clearly would raise questions on Code liability in that space.

- If the NCA believed they could not give a view and triaged DAML responses accordingly then again there is no legal defence, as far as we can see, for not subsequently proceeding with the payment once the NCA has responded to neither grant nor withhold consent. The only protection under POCA (that we can see) for not acting on the customer mandate would be for the NCA to withhold consent. That then potentially creates issues over repatriation and if the appropriate mechanism to return those funds to the victim is then subsequently through the

courts. In short, this would mean the NCA, as opposed to banks, becomes the main vehicle for freezing and returning the proceeds of fraud to victims.

- The NCA could of course choose not to respond, in which case it would seem each payment would be delayed for 5 working days until no response had been received. Even if in that period a firm was satisfied it was not fraud it could not make the payment.

POCA and Tipping Off

- In all the scenarios above if a firm subsequently, after submitting a DAML SAR, becomes satisfied there is not the risk of fraud they cannot make the payment until 'consent' has been granted. To further exacerbate the issue, there would be concerns over 'tipping off' in relation to explaining to customer, where enquiries may have been made, why a payment has not been made even though the bank is satisfied it is not fraud, whilst there is a DAML SAR awaiting a response.

POCA as a basis for repatriation of funds

- Nor do we see on the separate but linked issue how POCA can be used to provide legal cover for interfering with title – in our view it can only be used to provide a defence against money laundering.

- POCA creates clear mechanisms for the State to interfere with the right to property and in any case those mechanisms are restricted to the public sector, such as the courts. Even where the private sector is involved it is only on behalf of or in support of a relevant public sector body.

- We would be keen to avoid expectations on use of POCA in relation to repatriation, particularly on use of 'consent' as some firms have also taken the view they do not need to submit a DAML SAR when returning the proceeds of fraud. The NCA also changed a glossary code that supported that approach.

Annex D: Background on Banking Protocol

The Banking Protocol was developed in 2016 in response to the increasing risk posed by authorised push payments. Under the Banking Protocol scheme branch staff are trained to identify risk indicators which may suggest the customer is being scammed and, where necessary, to make an emergency call to Police.

Since its inception, the initiative has prevented in excess of £200million financial harm. Cases range from rogue traders who demand cash for unnecessary work on people's property, to courier scam fraudsters who persuade their victims take out a large sum of cash and hand it over to someone posing as a courier.

Recognising the success of the initiative, industry have continued to work with law enforcement, expanding the scheme to telephone and online banking, known as Banking Protocol Cross Channel (BPCC). The expanded initiative proposals delivers a police response to the homes of vulnerable victims who have attempted to make a payment via online or telephone banking which has been flagged as potentially being part of a scam.

Where transactions flag as suspicious and the PSP is unable to break the spell, customers are asked by the bank to visit their local branch to complete the transaction, enabling branch staff to carry out additional checks and use the Banking Protocol if necessary. However, if the customer is unable to visit their bank branch, for example if they are vulnerable or have a disability, staff are now able to directly alert the local police who will make a visit to the customer's home and assess

whether they have fallen victim to a scam. Until the police response is received the customers payment is held.
Early indications suggest this new approach is already proving successful, with one referral alone preventing the loss of £165,000 to a romance fraudster after the transaction was reported to police by telephone banking staff as a potential scam.

However, to gain law enforcement support for this initiative an SLA of 72hrs, from the point of the email referral submission to the responding officer reporting back to the referring firm had to be built into the process. Whilst the majority of BPCC referrals are completed within this referral time, some firms have been resistant to use the process due to the risks of going outside of the timeline allowed within PSR 17.