PAYMENTS STRATEGY FORUM CONSULTATION ON A BLUEPRINT FOR THE FUTURE OF UK PAYMENTS

RESPONSE BY THE FLA

SUMMARY

The Finance & Leasing Association (FLA) is the leading trade association for the UK motor finance, consumer credit and asset finance industries. FLA member companies include banks, building societies, the captive finance arms of manufacturers and various independent financial institutions. In 2016, members of the FLA provided £118 billion of new finance to UK businesses and households.

Below we respond to those questions that we and our members deem relevant and pertinent to their operations. We welcome the opportunity to respond to this consultation and hope that the response submitted in this format will be accepted by the Payments Strategy Forum.

We agree to be listed as one of the respondents to the consultation.

RESPONSE TO CONSULTATION QUESTIONS

Question 1.1

Do you agree with our recommendation to move towards a 'push' payment mechanism for all payment types?

Yes we do agree with a move towards push payment so long as this leads to clear reductions in transactional costs to associated payment products (such as Direct Debit).

Question 1.3

As a potential vendor, participant or user of the NPA, are there any other design considerations that should be included in the NPA, especially with regards to considering the needs of end-users?

We believe that careful thought will need to go into implementing measures that prevent payment fraud as part of the NPA.

As our members are service users they have seen first-hand how the Direct Debit scheme has helped facilitate fraudulent refund claims to the extent where, in some cases, a large number of Direct Debit payments have been refunded without any due diligence undertaken by paying banks to ascertain whether the claim was legitimate or not. The issue has no doubt been exacerbated by the time limitless Guarantee Direct Debit offers and inadequate scheme rules. We have been working with Bacs and the PSR to address these issues.

We would therefore recommend that any push payment method (and particularly Direct Debit) implements some form of verification process requiring the payee to securely verify the payment(s) that has been set up. Such a system must:

- Work smoothly for sale of goods and services both at the point of sale and online and should not create barriers to sales.

- Provide evidence beyond reasonable doubt that the customer verified the initiation of a Direct Debit – ensuring that malicious fraudulent customers who have verified a Direct Debit cannot claim they were unaware that it had been set up. Currently a counter claim / challenge system for service users is in place that relies on allowing recourse for fraudulent or incorrect claims based on the reason the customer gives. We have seen examples of where the system is being compromised by fraudsters who know how to approach the refund process in order to prevent paying banks from accepting counter claims or challenges. A verification process, if designed correctly, could ensure that a counter claim or challenge was automatically accepted by a paying bank and remove the need for a 'reason code' based system.

The NPA must also protect consumers against push-payment fraud. This is imperative to ensure there is confidence in the payment infrastructure. We understand the PSR are currently assessing the issue and looking at how various actors in the payment system can play more of a role in offering protection to customers. The consultation paper also describes the Financial Crime Data and Information Sharing solution and wider Improving Trust in Payments work. We would advocate the need for the PSF to continue to look at technological solutions that prevent fraud whilst continuing to enable the efficiencies that the NPA can offer.

We have previously raised concerns with Bacs and the PSR regarding how payment schemes such as Direct Debit can facilitate the proceeds of crime. This is an issue that no doubt exists for all payment products, whereby inadequate due diligence and compromised processes enable fraudsters to use the payment system to gain access to funds. We have seen examples of how Direct Debit fraud implicates the Direct Debit system in breach of the Proceeds of Crime Act (POCA). The NPA must seek to develop a system that ensures the payment products can evolve in line with both the requirements of POCA and payment service regulations.

Question 2.0

As a payee does your organisation serve customers who experience challenges paying regular bills?

a) Yes our members do.

b) Yes our members do experience cases where Direct Debits are cancelled, unpaid and in some cases fraudulently refunded.

There are a number of reasons why the above might occur and we list some examples below:

- Changing circumstances of a customer/payer – whereby they can no longer afford the monthly payments and therefore cancel their Direct Debit and go into arrears. The customer would often be reached and the lender might provide some flexibility to ensure payments can be brought up to date.

- The customer/payer does not recognise the Direct Debit – sometimes where the payment information provided on their account provides a different name to that of the organisation they agreed to pay. This would often be a communication problem that is easily resolved, the DD restored and payments brought up to date.

- Fraudulent activity – where the customer/payer has continued access to the underlying product or service purchased but knowingly cancels their DD and cuts off all lines of communication.

Question 2.2

Request to pay provides visibility to payees on the intentions of a payer. Would the increased visibility benefit your business?

If Request to Pay is used solely as a system that allows the customer to verify their Direct Debit then we agree it is helpful. However, such a system would need a fail-safe in place that protects from fraudulent abuse to ensure the Request to Pay message comes from a legitimate source and cannot in some way be manipulated.

We do not however feel that Request to Pay is suitable for ongoing requests and communication between the payer and payee for schemes such as Direct Debit. We think this functionality could lead to problems for payers and cause unnecessary conflict. We take no issue in payers requesting alternative pay dates for recurring payments and understand the need that payers have for flexibility, particularly in light of the UK possessing a flexible labour market that results in variable wage payment frequencies for many payers. Most of our members already allow the payment date to be changed typically after the first payment has been made.

However, we hold significant concerns where payers would request to make payments different to the value set out on an initial payment schedule they receive from the payee. The issue here is that the flexibility that Request to Pay would provide (if the requests were accepted by our members) could lead to payers falling into arrears, or forgetting that they had lowered the payment amount initially and had to pay higher payments towards the end of the agreement to satisfy its terms. If our members reject the requests then this could lead to conflict and a break down in the relationship between payer and payee.

The implementation of this functionality into the payment process could also lead to significant costs for our members and any service users that might be required to upgrade systems to facilitate its introduction.

Question 2.3

Request to Pay will result in increased communication between the payee and the payer. As a payee:

a) Would the increased communication present a challenge?

Yes (as explained in our answer to 2.2)

b) What benefits could you envisage from this increased communication?

None – some of our members already offer apps and personalised online accounts which enable payers to change the date they make payment on. Requirements for customers to change the amount they pay should be fully understood through a phone call or e-mail conversation. A messaging service therefore could potentially lead to the introduction of a redundant and unneeded communication channel between the payer and payee.

c) Do you see any additional benefits resulting from Request to Pay other than those described?

No

Question 2.5

We envisage payees stipulating a payment period during which the payer will be required to make the payment. As a payee, how do you think this payment period might be applied within your organisation?

If the Request to Pay also serves as verification and activation of a payment mandate then the first payment would need to be made at the point of sale (or when the sale of goods has transacted). Where the payment relates to taking possession of high value assets (such as vehicles, machinery, equipment etc.) the asset could not be released until the payee has verified that initial and future payments would be made.

Question 2.6

Request to Pay will offer payers flexibility over payment time as well as amount and method. As a payee:

a) Does your business model support offering payment plans and the ability for payers to spread their payments?

Yes. But as stated above, any adjustments to payment plans are made where the payee has good reason to help the customer in order to prevent detriment for particular circumstances. Not all payees are able to manage their finances effectively and need assistance that might require a conversation to be had with a trained customer adviser. There is also the case of where automating this process could lead to issues, such as where vulnerable customers are involved that might not fully understand how the process works.

b) Do you have a predominant payment method used by your payers?

Yes. Direct Debit. Feedback suggests that the vast majority of our members use this method but we cannot provide a percentage.

c) Do you offer your payers a choice of payment methods?

Yes. But this will depend on the company. Regular payments are typically taken using Direct Debit and early settlements/additional payments can be made using a debit/credit card, bank transfer and in some cases cheque.

d) Are there any incentives to use one payment method over another?

No. Not that we are aware of. As above, in most cases many of our members do not provide any choice of payment product used to make regular payments.

Question 2.7

A minority of payers may not be able to pay within the payment period. Through Request to Pay they will be able to request an extension to the payment period. As a payee:

a) Do you currently offer your payers the capability to extend a payment period, request a payment holiday or make late payments?

Yes. Some of our members do provide this flexibility but not all.

b) What are the conditions and eligibility criteria under which this is offered?

Conditions and eligibility vary by finance provider. As stated above such flexibility tends to only be provided where the payer makes contact with the payee and discusses their requirements. We are not sure what the Request to Pay messaging capability would offer over and above the standard communication channels between payer and payee.

Question 2.8

Request to Pay will offer payers the option to decline a request. The purpose of this option is to provide an immediate alert in case the request was received as an error or will be paid by other means. As a payee:

a) Would you find this information useful?

Yes. There are some scenarios where if a customer had made a Request to Pay in error then the ability to decline and communicate this through a message back (which allowed some explanation as to why the decline had been made) would be helpful. For example it would prevent unnecessary contact between the payer and payee to flesh out the issue.

b) Do you have any concerns about providing this capability?

Yes. We feel it should only be used where a payment is made in error. We do not take the view that a Request to Pay should be made that allows a payer to request a variation in the amount to be paid throughout the term of an agreement. We see Request to Pay only to serve as initial verification before the first payment (or one off payment) is made (and of all payments under a payment schedule agreed under the

mandate). If Request to Pay was rolled out for use at any time throughout a payment schedule, continuous requests to pay varying amounts, with continuous declines from payees, could lead to a break down in the relationship between both parties.

Question 2.9

Does the Request to Pay service as described address:

a) The detriments identified in our Strategy?

No. We take the view that in some cases the flexibility that Request to Pay seeks to provide a payer could lead to detriment if the payee allows the ability for the payer to change the amount they pay. Any perceived detriment to payers can already be addressed through standard communication channels with payers.

b) The challenges experienced by your customers? Does it introduce new challenges?

Yes. We have explained these above.

Question 2.10

As a payee, considering the information provided in this document,

a)b)c) Extent of change / challenges / timeframe:

This will depend on how Request to Pay is set up. Presumably there would be costs to payers interfacing with PSPs to provide the service and other technical changes to ensure information feeds through to databases and other systems. There might also be legal and resource considerations. It is difficult to provide any detail on timeframes, particularly as we do not yet have any refined specifications on Request to Pay.

Question 2.11

What are the features or rules that could be built into Request to Pay that would make it more valuable to your organisation for you to adopt it?

We note above that our members would see Request to Pay as a useful verification feature for initiating the first payment. Therefore for this to be successful it would need to be:

- generated instantly to work at the point of sale and not be subject to server delays or delay the payer/customer onboarding process.

- Resilient to fraud (including cyberattacks). Perhaps making use of dual verification technology such a one-time access code that is already in use by financial institutions and e-mail providers - in order to submit the Request to Pay.

- Easy to integrate for businesses using standard IT infrastructure and systems.

- Simple for payers and payees to understand and does not cause confusion and conflict.

Question 2.13

We recognise that additional work needs to be done in identifying potential safeguards including liability considerations associated with Request to Pay. As an end-user of Request to Pay:

a) What are some of the potential liability concerns that you may have?

We have outlined our concerns above.

b) Would you be interested in working with the Forum to define, at a high level, the liability considerations for Request to Pay?

Yes.

Question 2.15

We have presented two CoP response approaches (Approach 1 and Approach 2).

a) As a payer, what would be your preferred approach? Why?

We hold no firm view on this and potentially see issues with both approaches. However, Approach 1 is likely to be more plausible (in providing a clear answer) but only if the payee name applied to the CoP was restricted to the same defined list of payee names held against the account details, in order for the information to be matched against. i.e. the CoP payee name and account details name being matched against must be derived from and limited to the same source.

If approach 2 was taken and the payer was fed back details of the name of the organisation held, before the payment was pushed/submitted, then there could be confusion where the resultant account name fed back was different to the recognised name of the service or product provider the payer was expecting.

Questions 2.20-2.25

Enhanced Data

Our members have not provided any feedback on enhanced data. It is likely that the use of enhanced data will vary by business or stakeholder. However, if we do get the opportunity to work with the PSF we would reach out and ask our member companies to offer technical experts that can assist and provide feedback on this.

Questions 6.0-6.18

Improving Trust in Payments and KYC Data Sharing

The Payments Transaction Data Sharing and Data Analytics Strategic solution seems like a modern and collaborative way to tackle financial crime. The concept is certainly in line with the Government action plan for anti-money laundering and counter terrorist financing which outlines the importance of data sharing. There are obvious risks involved regarding where the data will be held, how it will be kept secure and ensuring

real time (or frequent) updates are achieved. Other difficulties will be around ensuring that all engaged stakeholders, such as law enforcement agencies, will also need to align their information to the data shared over the solution in order for financial crime and trends to be identified (particularly if this is to be done in an automated way). Governance of the development of the solution will also be key to ensure the project progresses in line with the timings given.

The KYC Data Sharing proposals look to provide a market solution to the prevention of financial crime associated with SMEs, however appropriate oversight to ensure fairness and competition in the KYC data sharing sector will be important.

Governance of payment schemes

It is worth us using this response to point out the need for governance of payment schemes set up under the current payment infrastructure. Evidence we have seen suggest that there is a need for the NPSO to review whether the rules of payment schemes should be scrutinised and supervised more closely prior to any new positive payment scheme developments that result from the NPA.

One example we can provide relates to Direct Debit and who ultimately decides to accept or reject counterclaims or challenges made by service users that disagree with refunds paid out to payers. Currently this decision rests solely on the paying banks. However, it is the paying banks that govern Bacs as a member organisation (being that the 15 largest banks are their core membership). This represents a significant conflict of interest. We have asked Bacs and the PSR to consider the implementation of an independent appeals process (or ring-fenced ombudsman/complaints specialist within Bacs) that can review counter claim or challenge decisions. Our members have, in the past, submitted challenges and counter claims that have been rejected on the grounds that signatures held by the paying bank, given by the suspected fraudulent customer, have not matched the signature held on the direct debit mandate. Rejection of a counter claim or challenge for this reason is irrational, since a fraudulent customer would make sure that signatures do not match. All other evidence in these scenarios has been rejected. There are also concerns over the level of knowledge held by individuals within paying banks that make such decisions (and where new staff enter this role). A paying bank also has an incentive to reject a challenge or counter claim since if they accept it they are liable for the loss of funds that has resulted in a Direct Debit refund from being paid out.

We would suggest the new NPSO looks at examples of this type of arrangement and considers the implementation of new Governance structures that leads to fair and impartial outcomes to this and similar issues.

Finance & Leasing Association – September 2017