



ADDRESS

2 Thomas More Square  
London E1W 1YN

WEBSITE

[www.financialfraudaction.org.uk](http://www.financialfraudaction.org.uk)

TO PSF (Payments Strategy Forum)

COPY FFA UK Members

## FFA UK RESPONSE

### PSF BEING RESPONSIVE TO USER NEEDS - DRAFT STRATEGY

Sep 2016

Consultation Title:	Being Responsive to User Needs
Representing (Self or Organisation/s):	Financial Fraud Action UK (FFA UK)
Address:	2 Thomas More Square, London E1W 1YN

**Please Check/Tick this box** if you don't want all or parts of your response to be published

### Declaration

"I confirm that our response supplied with this cover sheet is a formal response that the forum can publish, unless it is clearly marked 'Not for Publication'

## INTRODUCTION

Financial Fraud Action UK (FFA UK) is responsible for leading the collective fight against fraud in the UK payments industry. Its membership includes the major banks, credit, debit and charge card issuers, and card payment acquirers. Through industry collaboration FFA UK seeks to be the authoritative leader in defending consumers and businesses from financial fraud, by creating the most hostile environment in the world for fraudsters.

FFA UK's primary role is to drive collaborative action to reduce the impact of financial fraud and scams both across the industry, and with partners in the public sector, private sector, and law enforcement. It operates its own data and intelligence sharing bureau and sponsors a fully operational police unit.

### Key Comments

- FFA UK supported the creation of the Payment Strategy Forum. We believe it has great potential to provide an independent arena for different payment service providers and users to come together to agree priority areas for payment innovation. FFA UK representatives have been involved in three of the four supporting working groups: End Users, Financial Crime, and Horizon Scanning.
- The comments expressed by FFA UK have been developed through engagement with its members, however they are not representative of the industry/fraud community as a whole and are subject to change following a more robust evaluation of the individual solution proposals and clarity as to how they will each align with the direction of existing developments and measures the industry is already committed towards e.g. the EBA RTS (European Banking Authority Regulatory Technical Standards). The overwhelming response across members favoured this approach as without it; a more definitive stance is very difficult to provide. The proposals should be subject to proper impact assessment where the benefits for customers are clearly evidenced and proportionate against the costs of delivery by PSPs (Payment Service Provider); especially as these costs will ultimately be borne by end users.
- The PSF draft strategy largely focuses on changes to the UK interbank schemes which sit outside the remit of FFA UK. Therefore, we have limited our response towards the aspects related to the financial crime proposals. The BBA are expected to provide comment on financial crime relating to KYC (Know Your Customer) and Sanctions.
- There are strong concerns about the pace at which the forum is operating. PSPs require more time and engagement with the PSF to better understand the financial crime solutions and whether or not the intended benefits are proportionate to the investment, and the associated risks which include the interdependencies elsewhere requiring delivery by industry under regulatory and legislative mandate. Lastly, the number of changes proposed by the PSF constitutes a serious undertaking and may not be sustainable for smaller PSPs.
- We suggest the PSR should use the following tools to inform strategy-setting:
  - Wide-scale and in-depth consumer research. Consumers should continue to decide what works well for them and demonstrate this with their purchasing decisions.

- Market and technological research. Options for delivery should not be limited to those that are presented by representatives on the Forum/ working groups.
- Overview of regulatory and standard developments internationally, and particularly in Europe. If the PSR's aim is to grow competition it will presumably want the industry to be open to European providers, which will require a level of European interoperability.

## RESPONDING TO CONSUMER AND BUSINESS NEEDS

### 1. Do you agree we have properly captured and articulated the needs of End Users? If Not, what needs are missing?

Whilst user needs is not an area we are in position to provide a substantial and informed opinion on, we do feel strongly that the introduction of Assurance data (Confirmation of Payee) is widely supported as it will help to prevent commonly occurring cases of fraud where consumers and businesses are duped by fraudsters into making payments to unintended bank accounts/recipients. A robust evaluation of how the user needs were determined and the costs to deliver the solution verses the fraud savings it could bring to bear will be vital to attract the necessary investment from PSPs.

## IMPROVING TRUST IN PAYMENTS

### 5a Do you agree with our proposal regarding customer awareness and education? If not, please provide evidence to support your response.

Yes, a more coordinated approach is widely supported. A number of industry organisations are already tackling education and awareness (E&A) for their respective target audiences. However, the need for an overarching body to oversee the strategy towards these efforts would be welcomed and supported to ensure the following:

- Messages are consistent
- Avoid the overlapping of campaigns and inundating consumers with information
- More targeted campaigns
- Avoid duplication of effort
- Encouraging key stakeholders to participate and demonstrate the benefits of doing so

### 5b Do you agree the delivery of these activities should be through an industry trade body? If so, which one would be most appropriate to take the lead role?

Yes, we agree that activities should be delivered through an industry body. FFA UK has considerable experience in this space and has executed numerous successful campaigns, and would be well placed to deliver on the fraud related E&A activities described in the proposal. However, we recognise that some issues which will require E&A efforts will sit outside the remit of FFA UK and these should be delivered by whichever body is the most appropriate/reflects the interests of the target audience that the education and awareness is intended for. The Home Office Joint Fraud Taskforce could have a role in coordinating this.

**6 Do you agree with the establishment of guidelines for identity verification, Authentication and risk assessment? If not, please provide evidence to support your response.**

No, from the current understanding of the solutions which have yet to be fully costed and impact assessed it is not widely supported (see *bullet two under general comments*).

Each PSP has its own risk appetite and this varies even further across their respective payment types and instruments. Furthermore:

- Concerns were expressed towards common guidelines and standards impacting the ability of PSPs to innovate, stifle competition and impact the customer experience.
- Taking into consideration the significant resource and investment which will be required to deliver the solutions proposed it is still uncertain whether there will be any significant/proportionate benefits.
- Under PSD2 and the EBA RTS, PSPs will be mandated to adopt new standards for authentication the impact from which is yet to be fully understood therefore, the benefits of introducing further standards above and beyond this need to be fully justified and apparent.

More widely and strongly supported is the need for an effective mutual authentication mechanism over the telephony channel. There has been a significant rise in remote channel fraud across the industry and this can be attributed in large part to criminals exploiting the fact that users do not currently have an effective/robust means to authenticate their PSP over the telephone.

**7a Do you agree with our solution to develop a central data repository for shared data and a data analytics capability? If not, please provide evidence to support your response?**

Whilst the sharing of confirmed fraud data amongst PSPs and law enforcement is widely supported and welcomed the questions remains as to whether or not the benefit would be significant enough to warrant the time and investment. In addition, further details on the scope of the proposal are still required e.g. there is already activity in this space with the CDA (Cyber Defence Alliance), enhancements to FISS (Fraud Intelligence Sharing System) and CIFAS so how the proposal would fit in with these already existing efforts and investments needs to be better understood.

**7b Do you agree with the potential risks we outline? How should we address these risks? Are there further risks we should consider?**

Yes, data sharing is vital to protect consumers who are currently unnecessarily exposed to financial crime by the lack of sharing. The balance between this and consumer data privacy will be significant but equally as important is the integrity of data being shared. The following should be considered:

- Recourse of false/incorrect reporting, serious repercussions for the beneficiary account otherwise
- Ability to flag accounts where refunds were issued
- Development of reason codes
- Risk of liability from inadvertently passing on false/incorrect information

**7c If any legislative change is required to deliver this solution, would such change be**

**proportionate to the expected benefits?**

Yes, it is widely acknowledged that changes are required to existing legislation to accommodate the proposals and that it would be proportionate. More clarity/certainty towards this should be sought from Government prior to any attempts to change existing legislation.

**FINANCIAL CRIME INTELLIGENCE SHARING**

**8a Do you agree with our solution for financial crime intelligence sharing? If not, please provide evidence to support your response?**

Yes, intelligence associated with fraudulent payments is currently fragmented so PSPs at the sending or receiving end of the payment flow will only see a partial picture of the fraud incident. There is an obvious and pressing requirement for more comprehensive intelligence sharing and obligations on all PSPs to participate in it. Whether or not the solutions proposed are the most cost effective and beneficial approach to take is still unclear and requires further clarity on critical requirements such as the speed and mechanisms to share and agreed performance SLAs (Service Level Agreements) amongst participants.

**8c Do you agree with the potential risks we outline? How should we address these risks? Are there further risks we should consider?**

Yes, the risks are significant. In a similar way to criminal records, rigorous controls are required. Due to the significance of the risks associated with this data, it may be prudent to seek the involvement of an independent body/authority to oversee the use of the data and perform any necessary due diligence.

**8d Do the benefits of financial crime intelligence sharing outweigh the new potential risks created?**

There is no doubt that data and intelligence relating to fraudulent payments should be shared amongst PSPs. However, there are concerns towards the benefits of the proposed solution being outweighed by the costs of delivery. There could be an argument for cost saving by assessing the potential of improving existing financial crime intelligence sharing platforms as opposed to creating a new one.

**8e Can this operate without changes to legislation? If not, what changes to legislation would be required to make this happen? If any legislative change is required, would such change be proportionate to the expected benefits?**

Clearer guidance and interpretation to existing legislation should be sought as it could still be fit for purpose. A clear and unambiguous legal framework and ongoing due diligence is considered critical towards this proposal.

**8f What governance structure should be created to ensure secure and proper intelligence sharing?**

Self-regulation would be widely supported i.e. common standards for intelligence sharing overseen by a

relevant body. Many of the issues described sit within the sphere of the UK financial services regulator however, some elements go beyond for example where law enforcement is involved, and this needs to be taken into consideration when determining how the structure should be governed.

ooOOoo