Financial Services Consumer Panel
AN INDEPENDENT VOICE FOR CONSUMERS OF FINANCIAL SERVICES

Telephone: 020 7066 9346
Email: enquiries@fs-cp.org.uk

Financial Conduct Authority
12 Endeavour Square
London E20 1JN

30 April 2021

By email: cp21-03@fca.org.uk

Dear Sir/Madam,

Financial Services Consumer Panel response to CP 21/3 – Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual

Strong Customer Authentication Regulatory Technical Standards (SCA-RTS)

Introduction

The Consumer Panel is pleased that the FCA has identified the payments sector as a priority for the next three years and welcomes the opportunity to responds to CP 21/3. Technology is driving rapid innovation in the payments sector, revolutionising business models, transforming the ways in which firms engage with customers and reshaping consumer behaviour.

While we recognise the potential opportunities that these innovations create, we would caution that, to ensure these changes deliver real and durable benefits for consumers, it is imperative that consumers are at the heart of their design, development and delivery. The Panel would like to see the FCA challenge providers that fail to deliver consumer-centred services, for example by taking narrow technology- or purely profit-driven approaches to payments.

Payments are essentially about data, and confidence in the way that data is handled is central to confidence in payments. While access to data is at the core of change in payments today, it is key that widening access to sensitive data does not compromise that confidence.

It is therefore essential that consumer data is managed:

i. **Securely:** The process of authentication and consent, and how this is communicated between the customer, Third Party Providers (TPP) and Account Servicing Payment Service Providers (ASPSPs), must be highly secure. Rigorous fraud prevention mechanisms, and internal systems for securing data, must also be in place.
ii. **With full informed consent:** Consumers should be provided with clear information to maximise understanding and allow fully informed consent before their personal data can be processed. Consent must be obtained so as to prevent consumers from for example ticking a box, without becoming aware of the implications. It must also be as straightforward to withdraw consent as it is to provide it and TPPs should not continue to access the data of inactive consumers.

iii. **Transparently:** Consumers understanding of information such as how their data is being used, by whom and over what time period, is essential.

The design of the process for consumers to authenticate and provide consent for TPPs to access their data from ASPSPs must be bullet-proof and consent needs to be informed, rather than a tick box exercise.

The design should also be inclusive[1] and take into account the wide-ranging needs, behaviours and lived experiences of real consumers to ensure that services are accessible to, and usable by, the greatest number of people possible. This includes TPPs and ASPSPs consider the needs of consumers in vulnerable circumstances at all stages of the customer journey, as vulnerability can affect an individual's ability to assimilate information, make decicions, give informed consent and resolve problems, thereby increasing their propensity to suffer harm.

90-day reauthentication

Some level of friction for consumers is desirable to ensure data is accessed (i) securely (ii) with appropriate consent and (iii) transparently. The Panel nevertheless appreciates that the evidence shows re-authenticating every 90 days across all accounts may be too cumbersome for many consumers.

The Panel therefore supports the following proposals:

- Extending the re-authentication period, for example to six months or one year, as opposed to removing it entirely. If customers do not re-authenticate, TPPs cannot access their data, protecting inactive customers and those less digitally savvy.
- ASPSPs should issue reminders to customers every 90 days that their data is being accessed, including the terms agreed to and how to withdraw consent. It is most secure for customers to provide consent for TPPs to access their data directly to ASPSPs, where their data is held. It is essential that reminders are provided in such a way that minimises the likelihood of fraud.

Mandating the use of dedicated interface

The Panel supports this proposal.

Mandating APIs will reduce barriers to entry for TPPs, allowing them to offer a better service to consumers at a lower cost, and enabling providers to ensure greater security and data protection.

It is important that ASPSPs are strictly held to the 18 month timeframe stipulated, in order to ensure that consumers can truly benefit from these new services.

Prudential requirements

The Panel previously responded to the FCA's consultation `Coronavarius and safeguarding customers' funds: proposed guidance for payments firms'[1], and strongly supports this guidance being made permanent.

In addition to this guidance, it is important that strong and clear messaging is provided to consumers so that they properly understand what consent they are giving to whom, for what purpose, and with what level of protection.

[1] https://www.fs-cp.org.uk/sites/default/files/fscp_response_to_guidance_to_payments_firms_on_safeguarding_customers_funds_20200605.docx_.pdf

In the current economic climate and in this low interest rate environment, the risk of firm failure is high in the payments sector[2]. Therefore, it is more essential than ever that consumers are made aware of where FSCS coverage exists, and where it does not.

We would also urge the FCA to pay particular attention to firms' applications of its safeguarding recommendations and advocate the rapid implementation of HMT's proposed insolvency changes for payments and electronic money institutions.

Yours faithfully,

Wanda Goldwag
Chair, Financial Services Consumer Panel

[2] https://www.fca.org.uk/data/coronavirus-financial-resilience-survey-data