TEMPLATE: COMMENTS ON THE DRAFT "RECOMMENDATIONS FOR PAYMENT ACCOUNT ACCESS SERVICES"

Contact details (will not be published)	Mr. Farid Aliyev
	financialservices@beuc.eu
	+32 (0)2 789 24 01

☐	The comments provided should NOT be published

The table below shall serve as a template collecting comments received in a standardised way.

- Please **add** to the table **only issues where you consider that a follow-up is necessary**, i.e. no general statements like "We welcome the recommendations."
- All comments should be **separated per issue** concerned so that a thematic sorting can be easily applied later on. (i.e. one row for each issue).
- If needed, replicate page 2 for the provision of further comments.

The assessment form consists the four items which are suggested to be filled as follows:

- **Originator:** Name of the originator and ISO code of the country of the originator (e.g. NAME (AT/BE/BG/...))
- **Issue** (states the topic concerned): General comment, Scope, Terminology, REC 2, 1.1 KC, 3.2 BP, Glossary,
- **Comment:** Suggestion for amendment, clarification or deletion
- **Reasoning:** Short statement why the comment should be taken on board

Originator:

Name of the originator (e.g. name of the company or association)	BEUC, The European Consumer Organisation	**ISO code of the country of the originator**	BE

Comments on the recommendations for "payment account access" services

Issue	Comment	Reasoning
General comment	Amendment	BEUC supports the overall direction of the Recommendations, provided that third-party service providers (TPs) are regulated by the revised Payment Services Directive (upcoming legislative proposal) and all the essential issues linked to payment account access services (such as liability, which is out of scope of the draft Recommendations) are clarified, clearly defined and covered by the PSD. We believe the measures proposed by the draft Recommendations will considerably improve the security of payment account access services. That being said, in our view, the Recommendations do not sufficiently recognise and address the risks related to the operating model of some TPs: TPs – via their software – have access to consumer's personal credentials and use them to log into the internet banking application on the consumer's behalf. While the Recommendations are being addressed to trustworthy TPs which are currently operate on the market and wish to be regulated by the PSD, such operating models may seriously jeopardise the security of the payment system and consumer trust if in the future rogue traders will adopt them to defraud consumer bank accounts. With the exception of few Member States, payment account access services still have a small market share and this market will certainly attract the attention of fraudsters once it has reached important transaction volumes. It appears that even the payment account access services which do not require consumer to provide sensitive credentials are not secure enough, because account servicers' (banks') security systems are also vulnerable http://www.dutchnews.nl/news/archives/2013/04/dutch_internet_banking_problem.php http://news.idg.no/cw/art.cfm?id=3F6822FF-1A64-6A71-CE67724BB606D61C Furthermore we believe that, with such an operating model, consumer privacy becomes more difficult to maintain. For example, 11.2 BP provides that "*It is desirable that TPs only access data from the payment account expressly indicated by the account owner during the payment account access session, and not the account owner's other accounts, such as savings or securities accounts or other payment accounts*". It is unclear, however, how such a limitation will be applied to the above-mentioned operating model, since the TP access to the online banking application is not distinct from the consumer direct access without TP involvement. BEUC considers that TPs should not access consumer personal credentials as technically this is not a necessary prerequisite to providing payment account access services.
Objective of the Recommendations	Amendment	One of the objectives of the draft Recommendations is "*Increased transparency for account owners enabling them to assess risks and make an informed choice before and during the use of payment account access services*". This objective is unclear as it implies that when using payment account access services consumers run the risk of losing money or other risks. Payment services cannot be compared to the stock market where investors opt for more or less risk. All payment services offered to consumers must guarantee an adequate level of security and particular payment methods should not a priori entail more risk than others. Furthermore, how should an account owner (average consumer), who is not a payment services or IT expert, be expected to assess such risks? BEUC suggests that the above objective is amended accordingly.
Guiding principles	Amendment	Guiding principle (iv) of the draft Recommendations is to provide "*customer awareness and education programmes on security issues*". It would be more appropriate to use the term 'information' instead of 'education' because 'education' implies long-term investment which aims to change people's behaviour. Furthermore, consumers cannot be expected to become IT experts and a knowledge gap will always exist between the supply and demand sides. Consequently, under no circumstances should consumers be held liable for security incidents caused by the issues which are not under the full control of the consumer. BEUC suggests that guiding principle (iv) and other related provisions of the draft Recommendations are amended accordingly.

Implementation	Clarification	We welcome the binding nature of the Recommendations. Yet, clarification is needed regarding the sanctioning regimes, i.e. penalties which will apply for non-compliance with the Recommendations.
Recommendation 3: Incident monitoring and reporting	Amendment	3.2 KC provides that TPs and GAs (governance authorities) should immediately notify the competent authorities in the event of major security incidents with regard to the payment account access services provided. Consumers also should benefit from a mandatory data breach notification obligation: they should be immediately notified whenever there has been a breach putting their personal data at risk.
Recommendation 6: Initial customer identification and information	Amendment	In relation to providing consumers with information on "*inherent risks*" involved with payment account access services, please see our comments on 'Objective of the Recommendations' above. The draft proposal should be amended accordingly
6.2 KC	Amendment	As regards secure use of personalised security credentials, please see our 'General comments'. The draft proposal should be amended accordingly.
Recommendation 7: Strong customer authentication	Clarification	7.3 KC provides that "*The account owner's initial registration (if any) for payment account access services should take place in a safe and trusted environment, while taking into account possible risks arising from devices that are not under the TP's control*". This provision leaves room for different interpretations: 1) TPs should take measures against possible risks arising from devices that are not under their control; 2) TPs are not responsible for security incidents caused by devices that are not under the TP's control. If the second interpretation is correct, who would be held responsible in case of such incidences? As already mentioned above, consumers should never be held liable for security incidents caused by the issues which are not under their full control (web browser, antivirus software, etc). See our comments on 'Guiding principles' above. The meaning of 7.3 KC needs to be clarified.
8.1 KC	Clarification	"*The related procedures should be carried out in a safe and trusted environment, while taking into account possible risks arising from devices that are not under the TP's control*." Need for clarification as with 7.3 KC above
11.5 KC	Deletion	11.5 KC provides that "*TPs should not store sensitive payment data after the payment account access session of the account owner. TPs storing data should ensure that the data are appropriately protected against theft and unauthorised access or modification*". The second sentence should be deleted as it contradicts the first one and leaves room for interpretation. TPs do not need to store payment data after the payment account access session.
11.2 BP	Amendment	11.2 BP provides that "*It is desirable that TPs only access data from the payment account expressly indicated by the account owner during the payment account access session, and not the account owner's other accounts, such as savings or securities accounts or other payment accounts*". In our view, 11.2 BP should not be a recommendation but an obligation on TPs: Access should be strictly limited to payment transaction information; the TP should not be able to access other data visible on the payment account, e.g. payment transaction history of the account owner. Please also see our 'General comment' in relation to the operating model of some TPs where the TP logs into the internet banking application on the consumer's behalf.
Customer awareness, education and communication	Amendment	It would be more appropriate to use the term 'information' instead of 'education' (see our comments on 'Guiding principles' above).
12.4 KC	Amendment	According to 12.4 KC, consumers are expected to understand the need to "*check that any re-direction is to a secured website and that the extended validation certificate is drawn up in the name of a trusted entity, i.e. the account servicing PSP or the TP*". Please see our comments on 'Guiding principles' above and amend 12.4 KC accordingly.
12.6 KC	Amendment	12.6 KC provides that "*TPs should ensure that their liability regime is transparent to customers … including the maximum amount of indemnification in the event of unauthorised use/fraud …*" Liability and the amount of indemnification in the event of unauthorised use/fraud should be in compliance with the Payment Services Directive. 12.6 KC should be amended accordingly.
12.8 KC & 12.9 KC	Amendment	Please see our 'General comments' and amend 12.8 and 12.9 accordingly.