

**European Central Bank Public Consultation on**

**Draft Recommendations for the security of mobile payments**

**January 2014**

## Response from the European Blind Union

The **European Blind Union (EBU)** is a non-governmental, non profit making European organisation founded in 1984. It is one of the six regional bodies of the World Blind Union, and it promotes the interests of blind people and people with low vision in Europe. It currently operates within a network of 45 national members including organisations from all 27 European Union member states, candidate nations and other major countries in geographical Europe.

|  |  |
| --- | --- |
| **Contact details** | **Name of contact person: Carine Marzin****Email:** **ebu@euroblind.org** **or** **carine.marzin@rnib.org.uk****Phone number: +33 1 47 05 38 20** **EBU Office: 6 rue Gager-Gabillot 75015 Paris, France** |

We are happy for our contribution to be made public.

|  |  |  |
| --- | --- | --- |
| **Name of originator** | **European Blind Union** | **ISO codes:****BE, BG, CZ, DK, DE, EE, IE, EL, ES, FR, HR, IT, CY, LV, LT, LU, HU, MT, NL, AT, PL, PT, RO, SI, SK, FI, SE, UK** |

|  |  |  |
| --- | --- | --- |
| **Issue** | **Type of comment** | **Reasoning** |
| **Guiding Principles** | Amendment | Insert: ‘*Fifthly, MPSPs should ensure that strong customer authentication procedures are accessible for those disabled users who use assistive technology. It is important to take into account the fact that the user base for mobile payment services includes many older people and people with disabilities. Strong customer authentication procedures should not rely on user interface modalities and operations that these customers will find difficult or impossible to use.’*Reasoning: There are an estimated 150 million senior citizens in the EU and 80 million people with disabilities. The EU’s population is aging and the likelihood of living with a disability increases with age. Many EU citizens live with mild, moderate or severe impairments in vision, hearing, dexterity or cognition. To enable them to use mobile devices, they may use built-in or add-on access features such as spoken output of text, screen magnification or voice control. They may require information in alternative modalities, such as audible/tactile alternatives for visual information or visual/tactile alternatives for audible information. They may require user interface elements such as buttons to be sufficiently large and well spaced to allow for use by people with limited dexterity or hand tremors. Achieving accessibility for all customers is best achieved by ensuring that customer authentication procedures and user interfaces are developed according to the principles of Universal Design (<http://en.wikipedia.org/wiki/Universal_design> ) and evaluated by a diverse range of representative users, including older people and people with disabilities. |
| **Risk control and mitigation; Recommendation 4, 4.5 KC: ‘**MPSPs should also ensure that the data used by the payment application are not accessible to other applications/processes of the mobile device “application sandboxes’. | Clarification | It is important to clarify that the user interface for the payment application needs to be accessible via mobile devices’ built-in or add-on access technologies so any restrictions on the data must take this into account and user input must be possible with assistive software. Reasoning: If the application does not interact with the access technology, blind and partially sighted people are not able to use it. |
| **Risk control and mitigation; Recommendation 4, 4.8 KC**: ‘All changes should be subject to a formal change management process ensuring that changes are properly planned, tested, documented and authorised.’ | Amendment | Insert: ‘*Testing should cover the usability and accessibility of the mobile payment service user interface to ensure that it is fit for use by all customers. This should include evaluation by customers using the access technologies they rely on to use their mobile devices.*’Reasoning: All testing should include testing that addresses the needs of customers with disabilities and this should be done at the earliest stage when changes are made so that no customer is adversely affected by the changes proposed. |
| **Strong customer authentication; Recommendation 7: 7.1 BP** ‘Where a static password or PIN is used as an element to perform strong customer authentication for the authorisation of a mobile payment, the entry could be performed on an independent device’  | Clarification | It is important to clarify that the independent device needs to be accessible to blind and partially sighted users Reasoning: The independent device needs to provide voice output to a blind user so that they can interact with it otherwise they will not be able to use it and therefore carry out any mobile payments. |
| **Strong customer authentication; Recommendation 7, 7.2 BP:** MPSPs could provide solutions that enable customers to be aware of the activation of the payment interface of their mobile devices (such as a sound played by the mobile device each time a payment is authorised) | Amendment | Insert: ‘*A vibration should also be provided for deaf users at the same time as the sound’*Reasoning: Sound would not be accessible to deaf or deafblind users so an additional method should be used to cater for their needs. |
| **Strong customer authentication; Recommendation 7; 7.4 KC:** ‘Where a static password or PIN is used as an element to perform customer authentication MPSPs should ensure that the entry is performed in a way that prevents it from being compromised.’ | Clarification | It is important to clarify that whatever method is used to reduce the possibilities of the PIN being compromised, the process needs to be accessible to blind and partially sighted users. Reasoning: If the PIN entry is deemed to be compromised because a blind user would have the access technology read out the characters of their PIN as they are entering them, then there needs to be an alternative solution to render it more secure but also allow the user to check what has been entered. A possible solution would be to be able to detect if a screen reader is running and therefore present the user with the request to insert headphones/earphones in order to progress in the task of inputting a PIN. This would allow the user to still have the PIN spoken without it being compromised. The user should have the option to dismiss the reminder if they choose to do so. |
| **Authentication attempts and time-out; Recommendation 9: ‘**MPSPs should limit the number of log-in or authentication attempts (e’g’ wrong PIN entries), implement time out controls and set time limits for the validity of authentication.’ | Amendment | Insert: ‘*Time-out controls and time limits should be sufficient to allow an access technology user to find out the information that they are required to input and to then input it.*’ Reasoning: It takes longer for a user of access technology to navigate an interface and find out all the relevant information that is required and to then input the information, therefore a timed limit in which to achieve the task needs to take this into consideration. The user could be allowed to choose from a selection of time limits which one suits them. |
| **Authentication attempts and time-out**; **Recommendation 9, 9.3 KC:** ‘MPSPs should define the maximum duration after which inactive mobile payment service sessions are automatically terminated’ | Amendment | Insert: ‘*The maximum duration needs to take into consideration the needs of disabled users who might take longer to find the information they are required to input and then input it because of the nature of their access technology*.’Reasoning: A blind or partially sighted person navigating through an app will be interacting with it via access technology. However, the movement of the focus is not always communicated to the application as a user interaction and hence the user can find that a timeout has occurred even though they were reading through the page and accessing the data. If it is possible for the MPSP applications to realise that the focus movement via speech or magnification is a user interaction then this should resolve the issue but if this is not possible then the timeout must cater for someone using the application via access technology. |
| **Customer awareness, education and communication; Recommendation 12; 12.1 KC:** ‘MPSPs should provide at least one secure channel for ongoing communication with customers regarding the correct and secure use of the mobile payment service.’ | Amendment | Insert: ‘*This secure channel should be accessible, i.e. it should use communication methods that meet the needs of all customers, including those who are blind, partially sighted, deaf or hard of hearing. MSPSs should ensure that customer service staff is appropriately trained to ensure they have the knowledge, attitudes and skills to fully address all customers’ needs.* Reasoning: The customer base will always include a large number of people who are blind, partially sighted, deaf or hard of hearing, or live with other disabilities. Their needs must be taken into account. |

ENDS