Response to European Banking Authority consultation: Discussion Paper EBA/DP/2015/03

Dr Steven J. Murdoch
University College London
http://sec.cs.ucl.ac.uk/users/smurdoch/

January 2016

Strong customer authentication is important for preserving the security of payment systems, as well as for consumer protection. The authentication elements of strong customer authentication identified in the Payment Services Directive 2 (PSD 2) – knowledge, possession and inherence – need to be evaluated for both reliability and independence taking full consideration of the context in which the authentication technology is used. In particular, the level of security a particular authentication scheme can achieve depends not only on the abstract security properties of the technology (such as the cryptographic strength), but whether the technology's usability will allow a typical Payment Systems User (PSU) to actually follow the terms governing the issue and use of the payment instrument, so as to realise the full security potential when the authentication technology is used in the context of daily life.

An authentication technology which may in theory meet the criteria of strong customer authentication, but which is not sufficiently usable, will result in the PSU finding a way to bypass the limitations of the authentication technology by violating the terms governing the issue and use of the payment instrument, and therefore create increased risk of fraud. If such theoretically secure but practically insecure authentication technologies are allowed to be classed as strong customer authentication for the purposes of the PSD 2 then the PSU may be held liable for the full value of fraud losses, as set out in Article 74. Therefore the practical security of strong customer authentication, taking into account usability, is not only an issue for the security and integrity of payment services but also for protecting consumers.

Our recent research at University College London has examined the level of security offered by ATM cards, when used in conjunction with a PIN (thus meeting the possession and knowledge criteria of strong customer authentication). This research shows that UK bank customers are commonly asked to remember four or more different PINs, some of which they use every month at most. The combined effect of forgetting over time, as well as interference between the different PINs remembered, makes unaided recall of these PINs an infeasible task. Therefore customers engage in coping behaviour, such as writing down or re-using PINs, which reduce security and violate the terms and conditions associated with their card. As a result, customers who find that their card has been used without authorisation are usable to obtain a refund under the terms of the PSD, and the situation would be unchanged under the PSD 2.

The paper presenting and discussing these findings is "Are Payment Card Contracts Unfair?" presented at the 2016 Financial Cryptography conference, and published in Lecture Notes in Computer Science by Springer. This paper may be downloaded from http://sec.cs.ucl.ac.uk/users/smurdoch/papers/fc16cardcontracts.pdf

We would propose that Regulatory Technical Standards for strong customer authentication evaluate the security of authentication technologies not just from an abstract perspective where the PSU is assumed to be following the terms set out by the Payment System Provider (PSP) to the letter. Instead the technology should be evaluated as how it is actually will used by a typical PSU who is focused on performing the task at hand – making use of the payment system. Any authentication technology that requires excessive cognitive effort to meet its security requirements will not offer adequate security in practice and so should not be considered strong customer authentication. This usability evaluation should in particular take into account that the use of some payment instruments will be infrequent (thus exacerbating forgetting of knowledge elements), that in a competitive market PSUs will have payment instruments from several PSPs (thus creating interference between knowledge elements, and how the payment instrument is used) and that customers will follow security instructions provided through PSPs public communication channels rather than the fine-print of their contract with the PSP.

Further details can be found in the paper listed above.