To:
European Central Bank
Kaiserstrasse 29
60311 Frankfurt am Main
Germany

Dear Sir/Madam,

I am writing in response to the recently published "Recommendations for the Security of Internet Payments".

As part of the UK Financial Services sector we are members of a number of industry bodies - including UK Payments; Financial Fraud UK and the UK Cards Association. We have contributed to their responses to this paper and are supportive of their views, particularly those of Financial Fraud Action UK who have called out a number of difficulties with the approach proposed by the ECB - querying whether it is necessary at all as a separate initiative, as well as questioning many of the individual proposals

To reinforce these concerns we would like to focus on the following points as Lloyds Banking Group.

- There is ambiguity about who is, and more importantly isn't, in scope of this report. All institutions / entities involved in online payment services should be in scope of the recommendations including overlay providers who utilise the 'host' account to make payments. Restricting the scope of the recommendations solely to the PSPs ignores the big part played by other institutions and entities.

- More clarity is required in the definition of what the report means by 'strong customer authentication'. It needs to establish the principles that should support the claim for an authentication mechanism being declared as 'strong', rather than choosing just one possible definition and attempting to provide detailed requirements for that particular definition. It is over-simplistic to call two or three factor authentication 'strong'. Importance must also be placed on using the right combination of 'factors' in any given solution.

- The ECB suggest in their recommendations that a payment service provider may be held liable for any fraud loss in the event that stronger authentication is not used. Whilst this does not alter the current position for internet banking and card payments made over the internet via a 3D Secure enabled merchant, when a card is used in a non 3D Secure merchant the bank does not have the ability to connect directly with our customer and execute the 'stronger authentication' requirements and therefore could potentially be held liable for the losses. This would be a change from the current position as under the card scheme rules, for these non 3D Secure merchants, the card issuer has the ability to charge back the losses to the merchant as they are liable for any loss. It is noted that the paper does go on to outline some exceptions to the 'stronger authentication' principle but it does not explicitly cover the issue of when these exceptions can be used in the context of non 3D Secure enabled merchants and subsequent impact on liability for

fraud loss as outlined under current card scheme rules. Clarity on the above is required from the ECB and card schemes.

- Education and awareness activity should also be the responsibility of national Governments and Intergovernmental bodies as well as Internet Service providers and Payment Service providers.

- The assumption that card-not-present (CNP)fraud is solely linked to Internet payments is flawed as significant numbers of CNP transactions occur across non-Internet channels. CNP fraud is indeed the single largest fraud type in the UK but the total figure reported includes mail and telephone order fraud which would be unaffected by the implementation of the ECB recommendations. Estimates suggest that 63% of the total CNP fraud reported in 2011 was attributed to internet payments. This proportion has been declining in recent years as the industry introduces anti-fraud initiative, including the use of 3D Secure.

Yours Faithfully

Jane Attwood
Fraud Prevention Director
Lloyds Banking Group