

Benoît Cœuré: “Towards Retail Payments 2.0: The New Security Challenges”

Opening remarks by Mr Benoît Cœuré, Member of the Executive Board of the European Central Bank, at the joint European Central Bank/Bank of France conference “Towards Retail Payments 2.0: The New Security Challenges”, Paris, 22 October 2014.

* * *

Ladies and Gentlemen, dear conference participants,

First of all, I would like to apologise for not being with you today in Paris.

You all know the common fraud security check based on the fact that one person cannot be in two places at the same time. Unfortunately, I am no exception to this rule and so cannot be with you in person today, but I am pleased to be able to use this video message to share some of my thoughts on innovative payment methods and the challenges that they pose for central banks.

To begin with, I would like to recap some of the history of SecuRe Pay and why it was created.

Back in 2011, the standardisation of SEPA credit transfers and direct debits was well afoot, and cards had been migrated to the EMV standard.

However, we soon realised that the implementation of secure online payment methods was too slow, despite the fact that technical solutions were widely available. At the same time, we saw that Internet fraud was increasing.

The situation was particularly bad when it came to cards.

Our latest ECB card fraud report shows that 60% of fraud involves so-called “card-not-present” payments, mostly in the form of Internet payments.

Moreover, we observed that market pressure tends to make people take a race-to-the-bottom approach to security. Payment service providers fear that their competitors will use less secure but more convenient and cheaper solutions, thereby compromising too much on payment security.

With respect to fraud, I believe that this is only the tip of the iceberg.

In order to safeguard their reputation, many market players may have a tendency to understate major attacks or a high incidence of fraud to which they may have been exposed.

Moreover, we have come to realise that self-regulation has not been very successful in improving Internet payment security. We have to remember that it also took a very long to make point-of-sale payments secure.

For a central bank, whose task it is to promote the safety and efficiency of payment systems, this was quite a worrying trend.

And we were not the only ones to be concerned: according to the European Commission’s Cyber security report 2012, one out of every three European citizens had concerns about making payments online.

But the situation was not as serious in all countries.

A number of European countries had introduced minimum requirements for online payments, some as part of their oversight function and others as supervisors. Yet, these requirements were not harmonised and we needed to raise the bar for everyone.

At the same time, as some of you might remember, some banks complained to the ECB that some countries were imposing stricter security requirements than others.

For these reasons, we took the initiative to invite all supervisors and overseers within the European Union and the European Economic Area to form the European Forum on the Security of Retail Payments.

This Forum united the interests of two different parties: the interest of public authorities in the safety of payment services and the market's interest in homogenous requirements that allow for a level playing field.

SecuRe Pay was a big step forward and is also an excellent example of European cooperation.

It is a place where authorities can share their insights and discuss policies as well as the latest market developments. More importantly, we learn from each other and can agree on common minimum requirements. Thus, instead of leaving things in a grey area or duplicating efforts, the members of the Forum cooperate and optimise their resources.

Until today, the Forum has focused its efforts on new technologies and emerging risks, such as Internet and mobile payments and third party access to payment accounts.

The philosophy behind SecuRe Pay has been to try to develop generic requirements that can accommodate market developments and changes in technology. It also takes a risk-based approach.

For example, exemptions from the requirement of strong customer authentication measures can be made provided that the payment service provider carries out a sound analysis of the risk involved in a particular transaction.

Overall, the main changes brought about by the work of the Forum are that the industry will be obliged to have sound risk management, thoroughly identify and authenticate the customer and the transactions he/she wishes to make, protect sensitive payment information, upgrade their fraud monitoring tools and prevent fraud by educating the customer.

I believe that these measures are necessary and effective. They are also in line with market needs.

I would also like to point out that SecuRe Pay has provided substantial input for revising the Payment Services Directive.

Therefore, I think that as an initiative based on voluntary cooperation the Forum has been very successful and productive. In order to implement the developed requirements, however, some countries have needed a more formal legal basis.

In addition, the proposed Payment Services Directive envisages a number of mandates on security requirements for the European Banking Authority (EBA) to work on in close cooperation with the ECB.

Therefore, the Forum is now co-chaired by the EBA and the ECB. It formally supports both the European System of Central Banks and the EBA in their decision-making processes. The European Commission and Europol are represented as observers, and there is also dialogue with other authorities, such as the EU's Agency for Network and Information Security.

Cooperation, in particular between overseers and supervisors, is essential since they have complementary views, and not every country has the resources to build up its own know-how in this relatively specialised field. For example, one country might be more focused on IT and risk management, while the other focuses more on the payment system in general. Some authorities have mandates to look at investor and consumer protection, or competition, while others do not.

Yet we all share a common interest in maintaining trust in the security and efficiency of payment services.

These values are sometimes at odds with innovation.

Innovations – such as virtual currencies or payment account access services – can be disruptive. They may reveal where the inefficiencies of mainstream solutions lie and change the way we think about the “service aspect” of payments, but we should not forget that they often imply financial or security risks, which need to be weighed up against the benefits.

My philosophy is to learn from these solutions so as to make genuine payment services more secure and efficient. New players on the market are welcome so long as they are trustworthy and manage their risks adequately. They should not, however, put the end user or the security of other providers at risk.

Today is an excellent opportunity to discuss not only what the Forum has delivered and how it has successfully combined security and efficiency, but also the challenges that lie ahead for the security of retail payments.

I wish you a lively and interesting debate. Please use this opportunity to exchange your views with our experts. We constantly listen and learn from you and other security experts to shape our requirements.

Finally, I would like to thank all those who have actively contributed to this work. Please continue to make payments in Europe both more secure and more efficient.

Last but not least, a big “thank you” to the Banque de France and my colleagues at the ECB who worked hard to organise this event. Have a great conference.