Christian Noyer: "Towards Retail Payments 2.0: The New Security Challenges"

Opening speech by Mr Christian Noyer, Governor of the Bank of France and Chairman of the Board of Directors of the Bank for International Settlements, at the conference "Towards Retail Payments 2.0: The New Security Challenges", Paris, 22 October 2014.

* * *

Ladies and gentlemen,

I am delighted to open this conference today, dedicated to the work of the Secure Pay forum and to the new security challenges that lie ahead for retail payments. On behalf of the European Central Bank and of the Banque de France, I would like to welcome you all in Paris, and thank you for accepting our invitation to participate to this event. All the authorities that have an interest in the area of security at national and European level are represented today together with the major stakeholders of the private sector. I have no doubt that this will favor fruitful debates and a comprehensive overview of major challenges and issues regarding the security of retail payments.

This conference organized here in Paris illustrates the continuous support that the Banque de France has been providing to the Secure Pay forum from the very beginning, in order to promote the best practices in the field of security for retail payments in Europe.

This support has its roots in the Banque de France's mandate which, since 2001, explicitly requires that we ensure the safety of cashless payments. This has contributed to fuel a long-standing experience in addressing safety and efficiency issues and trade-offs from a public policy perspective that I would like to refer to, in order to draw a few lessons that you might be willing to consider in the course of the debates you will have today.

Over the past decade, the financial sector has changed considerably with the emergence of the Internet and the use of new information technologies. This is particularly true for payment means. The introduction of chip and PIN in France in the early nineties, and then all across Europe in the past few years is a great example of how innovation can bring about efficiency but also safety benefits to the payments chain. Such introduction has indeed contributed in making card payments highly secure at the point of sale.

However, innovations have also brought about new challenges in terms of risks to address. This is notably the case with the development of distant payments allowed by the Internet. As underlined in the report on card fraud published by the ECB in February 2014, fraud on "card not present" transactions, mainly via the internet, increased by nearly 21% in 2012 in the SEPA area, and accounted for 60% of all fraud losses on cards issued inside the SEPA.

Fortunately, the vulnerabilities at the root of those frauds are well identified and important efforts are underway both by public authorities and the private sector to address them. In France an important contribution comes from the "Observatory for payment cards security", which I have the pleasure to chair. Its recommendations have facilitated the recognition by stakeholders, who are all represented in the Observatory, of the importance of strong customer authentication for Internet payments and facilitated its wide adoption. This has significantly contributed to limit the impact on fraud rates, at least for national payments, and it has helped foster the dramatic expansion of e-commerce that we currently see.

But beyond the development of card payments via the Internet, other innovations such as mobile and contactless payments or online banking services also raise important issues. These issues notably include the protection of sensitive payment data. To address them, the Banque de France has been working with the banking community, which translated into an agreement in 2011 to promote the protection of bank account identifiers and card numbers. This issue of protection of sensitive data appears all the more important to address that we

witness the entry of newcomers in the payment chain like third party payment services providers, who may contribute positively to foster innovation and potentially competition in the retail payments market but whose modus operandi should not lead to lower the current security level of online banking services.

What lessons can we draw from that experience to promote best practices in the field of security for retail payments on a larger scale? I would like to underline three of them which might be of interest for your debate today:

First, consumer uptake of innovative payment solutions is all the more large and sustainable that those solutions are safe and it is in the innovators' interest to pay enough attention to security issues.

Second, the dialogue and the cooperation between the stakeholders in the security of payments is a must to obtain solid results. Forums like the French "Observatory for payment cards security" which gathers merchants, consumers, banking and payment markets stakeholders, but also representatives from the French Parliament and other relevant public authorities may prove quite helpful from that perspective. In that kind of forums, authorities have an important role to play as catalysts in order to facilitate consensus between players, to overcome technical issues and to adopt requirements which will ensure the highest security of retail payments while encouraging innovation and efficiency.

Lastly, cooperation and coordination between public authorities with responsibilities in the field of payments safety need to integrate a European and international dimension to be fully effective. This is a direct consequence of the European and even global interdependencies of security issues. I am happy to see that at European level, the creation of the Secure Pay forum in 2011 has followed this path by reinforcing cooperation between central banks and prudential authorities of the European Union and the European Economic Area in the field of retail payment security. This cooperation within Secure Pay has already delivered important results: two sets of recommendations have been issued so far, concerning the security of internet payments in 2013, with an expected compliance of the market by February 2015, and the security of mobile payments in 2014, with recommendations currently being finalized. The final text of the recommendations concerning the security of payment account access service has also been published for information in May 2014 and shared with the EBA, in light of the ongoing revision of the Payment Services Directive. The fact that the European legislator has taken into account large parts of the Secure Pay forum's recommendations in the review of the Payment Services Directive is for me the proof of the quality of the works led by the forum. I particularly welcome the integration of strong customer authentication in the revised text of the directive, which clearly constitutes a major progress in the security of retail payments.

Secure Pay has recently undergone a significant governance change, and will in the future be co-chaired by the European Banking Authority and the European Central Bank. This should further increase cooperation between the oversight and supervision institutions and ease the implementation of recommendations.

To conclude – and I will finish there –, I would like to underline how topical this conference is. As the proposal for the revised Payment Services Directive is currently discussed in the Council of the European Union, a unique opportunity is given today to all stakeholders to tackle the different issues raised by the new regulation in the presence of representatives from all European competent authorities that are involved.

Once again, thank you all for being here, and I wish you fruitful and vivid discussions on all of these aspects, hoping this conference will provide you with a comprehensive overview of the new security challenges for retail payments.

Before leaving the floor to our first set of panelists I now invite you to listen to Benoît Cœuré, Member of the Executive Board of the European Central Bank, who cannot be physically with us today but who has recorded his comments for us.

Thank you for your attention.