EUROPEAN CENTRAL BANK

EUROSYSTEM

PUBLIC NOTE ON SECURITY OF PAYMENT ACCOUNT ACCESS SERVICES

1 BACKGROUND

E-commerce is a rapidly growing and globally expanding industry and has the potential to spur overall economic growth. The security of payments when buying and selling goods or services offered through the internet or other communication networks has become a matter of concern for central banks. Ensuring the smooth operation of payment systems is one of their basic tasks. Safe and secure functioning payment systems are important for building and ensuring trust in a currency. Clarifying security requirements and extending them to new players on the market, who should be subject to appropriate supervision, will strengthen the overall security of the payment system.

This is the context in which, at the end of 2010, the ECB took the initiative to set up the European Forum on the Security of Retail Payments (the "Forum").[1] The Forum is composed of EU central bank overseers and banking supervisors. Its objective is to facilitate common knowledge and understanding of issues related to the security of electronic retail payment services and instruments and, where necessary, issue recommendations.

As its first achievement, the Forum released in January 2013 a final and comprehensive set of "Recommendations for the security of internet payments". The services covered by these recommendations include - irrespective of the device used - the execution of card payments on the internet, the execution of credit transfers on the internet, the issuance and amendment of direct debit electronic mandates, and the transfer of electronic money between two e-money accounts via the internet. Harmonised security recommendations for these services constitute an important step in the fight against payment fraud and contribute to increased consumer trust in internet payments.

The internet payment recommendations exclude so called payment account access services, in which an account holder uses a third-party provider (TPP) to access his/her payment account to initiate a payment or to obtain account information. Given the distinctive features of payment account access services, the Forum decided to address them separately.

[1] The final mandate was agreed in May 2011.

In broad terms, payment account access services include account information services and payment initiation services:

- *"account information service" means a service in which a payment service user makes use of a TPP to receive consolidated information on one or several payment accounts held by the payment service user with one or several other payment service providers.*
- *"payment initiation service" means a service in which a payment service user makes use of a TPP to initiate a payment from the account the user holds at another payment service provider (PSP).*

In practice, payment account access services are gaining increasing market traction and payment initiation services are already among the most important payment methods for e-commerce transactions in some Member States. The specific nature and risks of these services arise from the involvement of at least one additional entity in the payment chain and its interplay within the processing architecture of electronic retail payment services. The Forum welcomes the proposal of the European Commission to extend the Payment Service Directive (PSD) scheme to cover payment account access services and their providers. The extension of the current list of payment services to include payment initiation services and account information services is seen as a way to support innovation and competition in retail payments. The Forum expects new entrants on the market to provide security in their payment solutions on the same level as the existing market entities.

2 OUTCOME OF MARKET CONSULTATION

In January 2013, the Forum launched a public consultation on a set of draft recommendations for the security of payment account access services. In total, 38 responses were received. The responses are published on the ECB's website together with this note, except when the respondent indicated that its response was not for publication. The comments were mostly made by European and national banking and payment associations. A few individual credit institutions, TPPs and consultancy companies also provided feedback.

MAIN OUTCOME

In general, the respondents welcomed the Forum's initiative of drafting recommendations for payment account access services and appreciated its transparency in consulting the public. The main issues raised in the consultation included, among others, the need for contracts, liability

issues and the sharing of credentials. The Forum considered all contributions carefully and has drawn from its work the following main conclusions:

- *The Forum supports the proposal that TPPs should be licensed and supervised*
- *TPPs and account servicing PSPs should ensure mutual authentication when communicating in the context of providing payment account access services.*
- *The non-sharing of the personal user credentials with the TPP would address the security concerns by some of the current interactions between TPPs and AS PSPs.*
- *Third-party payment service providers should ensure that customers are appropriately authenticated by relying on strong customer authentication*[2].
- *TPPs' access to information on payment accounts should be limited to the minimum they need for their activity. For payment initiation services, access by the TPP to payment accounts means receiving from the account servicing PSP notification of the delivery of the payment order and information on the availability of sufficient funds for the specified payment transaction.*

Mutual identification and authentication

TPPs and account servicing PSPs should ensure mutual authentication when communicating in a secure way in the context of providing payment account access services. This can be achieved through agreed technical arrangements or the adoption of a suitable standard protocol. The same requirement would apply to the communication between TPPs and e-merchants.

A common European standard

A number of respondents to the public consultation on the draft recommendations, including consumer protection organisations, corporate and banking associations, payment schemes and account servicing PSPs, pointed out that certain risks, i.e. identity theft, cannot be ruled out in payment initiation and account information services, as with all all online banking services, even if the proposed recommendations were to be fully implemented. The root causes of these risks arise from the use of the customer online banking interface and the related sharing of personal user credentials with the third-party payment service provider. After careful consideration, the Forum came to the conclusion that the most appropriate way to mitigate these risks would be the development of a solution in which the TPP ensures strong customer authentication for the initiation of payments or access to account information through either of the following two ways:

[2] Strong customer authentication is also required in the "Recommendations for the security of internet payments" and in the draft "Recommendations for the security of mobile payments".

1. *redirecting the payment service user in a secure manner to his/her account servicing payment service provider for such authentication. This means the payment service user's personalised security features issued by the account servicing payment service provider are not shared with the TPP, or*
2. *issuing its own personalised security features for such authentication.*

To this end, the Forum recommends the development of a new European standard.

The Forum recommends the development of an open standard for communication between TPPs and account servicing PSPs, which would allow consumers to use any TPP to access any PSP throughout the EU. In addition, this standard should define the redirection procedure and the account servicing payment service provider's interface that allows the consumer to authorise the payment. This standard could be defined by the European Banking Authority (EBA) in close cooperation with the ECB and following consultations with the relevant stakeholders. It could include technical and functional specifications, as well as related procedures and in particular expectations on 24/7 availability of the interface and swift response times for the authentication. Standardisation is a normal part of European market integration and further developments should allow the industry to rely on a secure common standard that allows strong customer authentication by the account servicing PSP. This would reduce the technical workload for TPPs, foster innovation and, at the same time, ensure trust in safe and efficient payment services. The standard should be finalised shortly after the entry into force and prior to the transposition date of the PSD2 and thereby ensure that all elements of the Forum's recommendations can be applied at the same time. It should be noted that, whereas all PSPs will be obliged to offer the European standard, TPPs may nevertheless continue offering solutions based on a secure proprietary standard provided that it complies with all the recommendations.

The Forum believes that the solution it proposes has the merit of reconciling *security* - which is the focus of its work - with *innovation and competition* - through supporting TPPs' right of access to payment accounts as proposed by the European Commission in its July 2013 proposal - and *market integration* - through the development of a common standard. The solution requires amending some of the security-related provisions of the Commission's PSD2 proposal. The Forum believes that its solution is one that is viable and the best suited to meet in full the objectives of ensuring a high standard of security while being congruent with the notions of innovation and competition. While promoting its favoured model, the Forum remains open to alternative options should these be proven to strengthen the overall security and efficiency of the payment system more effectively.

2.1 OTHER COMMENTS

Other main comments from the public consultation include the following.

Contractual agreements between TPPs and AS PSPs

Many respondents, including banking associations, payment schemes and PSPs, raised the question of contractual agreements between TPPs and account servicing PSPs and supported contracts as a mandatory condition to allow the TPPs access to payment accounts. The Forum is of the opinion that contracts between the account servicer payment service providers and the TPPs are one possible option (other options include a multilateral scheme and/or industry standards) to clarify a number of important aspects related to the provision of payment account access services provided that they are not misused on unfair and unjustified grounds. This qualification stands in line with the ECB legal opinion on this matter.

TPPs and governance authorities of schemes

Payment account access services can be offered as proprietary solutions by individual TPPs or they can be organised in the form of a scheme, with a governance authority (GA) and TPPs - and usually account servicing PSPs - as the scheme's participants. Contrary to what some respondents in the public consultation may have perceived, the Forum is of the opinion that both solutions should be treated in the same way when defining security requirements.

3 THE WAY FORWARD

The proposal for the new PSD that the European Commission published in July 2013 - after the Forum launched the public consultation on its recommendations for payment account access services - includes a mandate for the European Banking Authority (EBA) to develop guidelines on security measures, which include these services. This led the Forum to decide not to publish the final text of its recommendations as this could create confusion in the market. The Forum will instead transmit its final text to the EBA. The Forum expects that, in practice, the latter will draw heavily on the work of the Forum. The core elements of this work are reflected in the present note.