EUROPEAN CENTRAL BANK

EUROSYSTEM

RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS: OUTCOME OF THE PUBLIC CONSULTATION

1 INTRODUCTION

In response to the widespread experience of regulators that payments made over the internet are subject to higher rates of fraud than traditional payment methods, the European Forum on the Security of Retail Payments, SecuRe Pay (the "Forum") has developed "Recommendations for the security of internet payments". The recommendations were submitted for public consultation from mid-April to June 2012 and the overall market feedback was very positive.[1] Comments were received from 59 respondents in 17 EU countries and included both European and national associations and authorities. This note summarises the main concerns and issues raised in the public consultation.

2 RATIONALE FOR RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

Some respondents called for very limited supervision and/or oversight of internet payments. A few even submitted that internet payments should not be regulated at all. Oversight and/or supervisory frameworks for internet payments already exist in many countries, most of which are based on the Basel Committee's Risk Management Principles for Electronic Banking,[2] or derived from oversight standards for payment instruments[3]. The security of retail payment systems, services and instruments is important for both maintaining confidence in the currency and the smooth functioning of the economy. While some actors have developed effective and customer friendly security measures or standards on their own initiative, the security requirements applicable to internet payments need to be harmonised and further enhanced to reduce vulnerability to and the likelihood of fraud.

Other respondents suggested that a cost-benefit analysis of the recommendations would be useful. However, the Forum believes that such an analysis is not needed. The recommendations are the result of detailed discussions, thorough analysis and the authorities' day-to-day experience.[4] The Forum members considered all of the comments carefully before finalising the text. Furthermore, the recommendations are formulated as generically as possible to take into account continual technological innovation and an ever-growing array of internet payment products and services.

Existing oversight and/or supervisory frameworks will be updated and harmonised based on the recommendations.

3 SECURITY AND CUSTOMER CONVENIENCE

Concerns were expressed as to whether the recommendations preserve an appropriate balance between security and customer convenience. The Forum points out that the recommendations are

[1] All of the comments received are available on the ECB's website, unless an individual respondent expressly requested otherwise (http://www.ecb.europa.eu).
[2] Basel Committee on Banking Supervision (2003), *Risk Management Principles for Electronic Banking*, July.
[3] European Central Bank (2009), *Harmonised oversight approach and oversight standards for payment instruments*, February.
[4] The need to implement adequate security measures is highlighted, inter alia, in the ECB's report on card fraud (July 2012).

based on a proper assessment by payment service providers (PSPs) and payment schemes of the risks involved. This risk-based approach is aimed at enabling the security of those transactions most at risk to be improved, while at the same time preserving user convenience. Moreover, the recommendations should be seen as minimum requirements, which leave a certain degree of freedom on how to implement them in practice. They are neutral as regards the means (i.e. the technology) to be used. Similar security requirements have already been implemented – at least partly – in several Member States, with satisfactory customer experience.

4 DEFINITION OF STRONG CUSTOMER AUTHENTICATION

Many of the comments received related to the definition of strong customer authentication, about which there appeared to be some misunderstanding. The definition of strong authentication used by the Forum incorporates well-known security concepts. Some respondents did not appear to consider the definition as an overall concept but referred only to parts of it. Others suggested including additional elements, which would arguably bring excessive detail to the definition and thereby weaken it. Overall, the Forum concluded that there was no need to amend the definition of strong authentication.

5 REFERENCE TO EXISTING STANDARDS

A number of respondents suggested including more specific references in the recommendations to existing standards. Others disagreed with the examples given. In developing the recommendations, the Forum deliberately chose not to set specific security or technical solutions, nor redefine, or suggest amendments to, existing industry technical standards or the authorities' expectations in the areas of data protection and business continuity. Specific technical solutions are to be addressed by the PSP itself and standard-setting bodies as technology evolves. The draft recommendations submitted for consultation did contain some (non-exhaustive) references to existing standards, which were given merely as examples of solutions used in the market. These references have been removed from the final version of the recommendations. Nevertheless, when assessing compliance with the security recommendations, the authorities may take into account compliance with the relevant international standards.

6 IMPLEMENTATION ISSUES

Many of the inquiries related to whether the minimum requirements would create a level playing field. This calls for two comments. First, the Forum members are committed to integrating the recommendations in their existing supervisory and oversight frameworks and implementing them in a way that is consistent across jurisdictions, based on a common methodology. Second, the geographical scope of the recommendations corresponds to that of the Payment Services Directive,[5] namely the European Economic Area (EEA). The proposition to expand this scope to "one-leg out" transactions[6] is part of the ongoing discussions on the review of the Directive.[7] The Forum members intend to promote the recommendations to authorities outside the EU/EEA and when cooperating

[5] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, p. 1.

[6] Transactions where one of the PSPs is located outside the EEA.

[7] Article 87 of the Payment Services Directive requires the European Commission to present a report on the implementation and impact of the Directive including, inter alia, the possible need to extend its scope.

with international organisations, such as the Bank for International Settlements, the International Monetary Fund and the World Bank.

A number of respondents questioned the suggested implementation date. Upon careful consideration of the relevant arguments, 1 February 2015 has been set as the date by which the recommendations should be implemented by PSPs and governance authorities of payment schemes.

7 CONSISTENCY WITH OTHER EU LEGISLATION

Some respondents outlined potential conflicts with anti-money laundering law with respect to simplified customer due diligence. The Forum has clarified that the recommendations are without prejudice to existing EU legislation in this field.

Issues were also raised with respect to data protection legislation. Data protection is outside the scope of the Forum's work. However, the Forum believes that the processing and exchange of data on suspicious transactions, IP addresses[8] and accounts is necessary in order to detect, analyse, prevent and stop malicious attacks on internet payment infrastructures. It also facilitates the reversal of fraudulently initiated payments. Any processing and exchange of such information must, of course, take place in a secure environment and between trusted and duly identified parties.

8 FUNCTIONAL SCOPE

A number of comments from market participants have led the Forum to extend the scope of the recommendations to cover business cards, all types of direct debit e-mandates and transfers of electronic money between two e-money accounts. Payment account access services provided by a third party are not covered by the recommendations. Given their distinctive features, they will be the subject of a separate report.

9 APPLICATION OF THE RECOMMENDATIONS TO CUSTOMERS AND E-MERCHANTS

A number of comments suggested inserting recommendations applicable to e-merchants and customers. By providing payment services to e-merchants, PSPs allow them access to the payment infrastructure and potentially to sensitive payment data, which could be a source of security risk. Thus, PSPs should contractually require e-merchants to comply with the necessary security requirements. Some of the relevant recommendations have been amended in the interests of clarification. Beyond that, the Forum can only suggest best practices. The report also differentiates between e-merchants that are willing and have the means to take on fraud management at a level comparable to PSPs and others that use ready-made packages from PSPs. The latter are assumed to have relatively little expertise in the security of internet payments, as are certain types of customer, i.e. consumers or micro-enterprises. Although some respondents suggested that recommendations should be developed to apply to customers, this is outside the Forum's competence. The Payment Services Directive outlines customer liabilities and any necessary clarifications in this respect should be covered by the review. It is the task of PSPs to deliver professional customer services and take into account all of the related risks.

[8] An IP address is a unique numeric code identifying each computer connected to the internet.

Address:
Kaiserstrasse 29,
60311 Frankfurt am Main,
Germany

Postal address:
Postfach 16 03 19,
60066 Frankfurt am Main,
Germany

Telephone: +49 69 1344 0;
Website: http://www.ecb.europa.eu;
Fax: +49 69 1344 6000