NATIONAL BANK OF THE REPUBLIC OF MACEDONIA
5TH CONFERENCE ON PAYMENT AND SECURITIES SETTLEMENT SYSTEMS

SECURITY OF RETAIL PAYMENTS

Ohrid, 5 June 2012

Rui Pimentel
Payment Systems Department
Banco de Portugal

Banco de Portugal
EUROSYSTEM

AGENDA

1. Involvement of Central Banks in retail payment systems
2. Creation of the SecuRe Pay Forum
3. Recommendations for the security of internet payments
4. Main focus & outlook

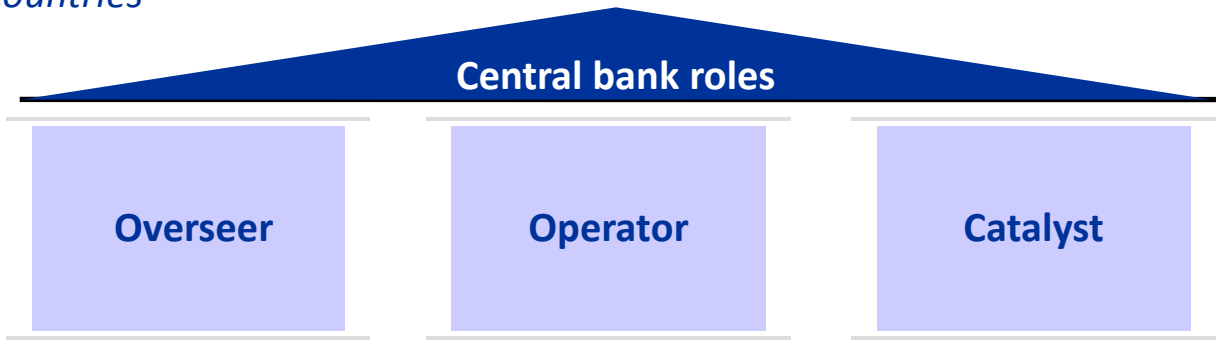
1. INVOLVEMENT OF CENTRAL BANKS IN RETAIL PAYMENT SYSTEMS

1. INVOLVEMENT OF CENTRAL BANKS IN RETAIL PAYMENT SYSTEMS

The safety and efficiency of retail payment systems and instruments are important for maintaining confidence in the currency and promoting an efficient economy

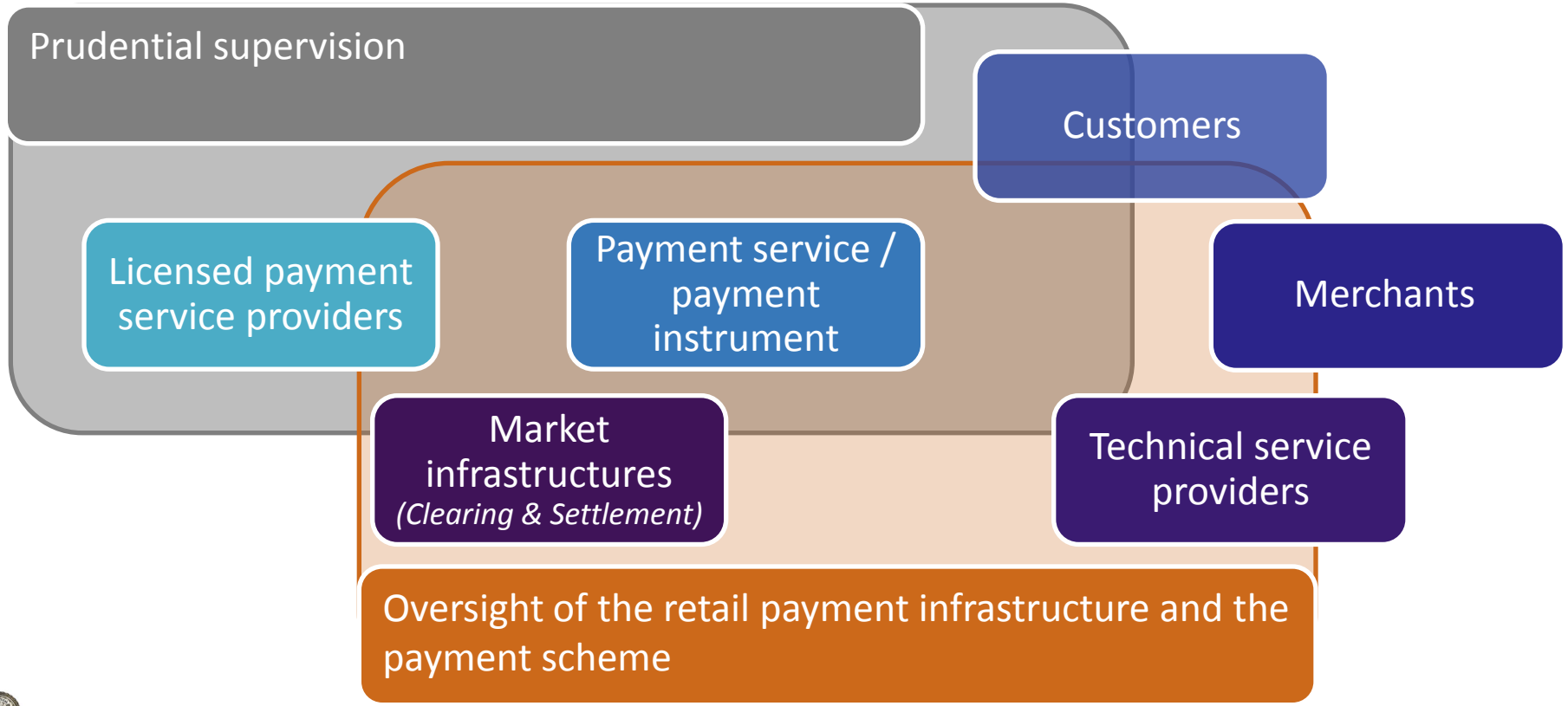
Legal basis:

- *Article 105 (2) of Treaty and Article 3 of Statute: "the basic tasks of the European System of Central Banks (ESCB) include the obligation to promote the smooth functioning of payment systems"*
- *Article 22 of the Statute: "The ECB and NCBs may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payment systems within the Community and with other countries"*



1. INVOLVEMENT OF CENTRAL BANKS IN RETAIL PAYMENT SYSTEMS

Retail payment services involve many actors



2. CREATION OF THE SECURE PAY FORUM

2. CREATION OF THE SECURE PAY FORUM

In the context of growing relevance of security aspects in the agenda of Central Banks regarding retail payments issues, the ESCB set up the European Forum on the Security of Retail Payments (SecuRe Pay Forum) in February 2011

→ **Voluntary cooperation between entities in charge of oversight & prudential supervisors in the EU / EEA; European Commission and Europol participate as observers**

- ❑ Establishment of common knowledge and understanding with regard to electronic retail payment services, instruments & PSPs
- ❑ Address major security weaknesses and vulnerabilities
- ❑ Harmonized recommendations

2. CREATION OF THE SECURE PAY FORUM

As a newly established structure, the SecuRe Pay Forum focused on the main objectives of its charter during the first year, namely the definition of recommendations for the security of internet payments

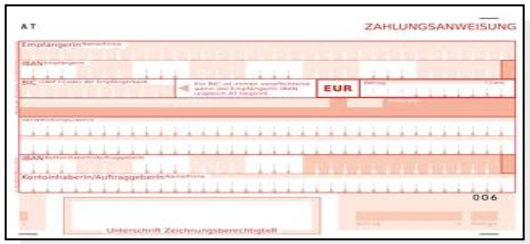
→ **In this process, the dialogue with market representatives was fostered, as a way of gathering relevant information about initiatives and knowledge in this field**

→ **As a result, the draft recommendations were published on 20 April 2012 and are in public consultation until 20 June 2012**

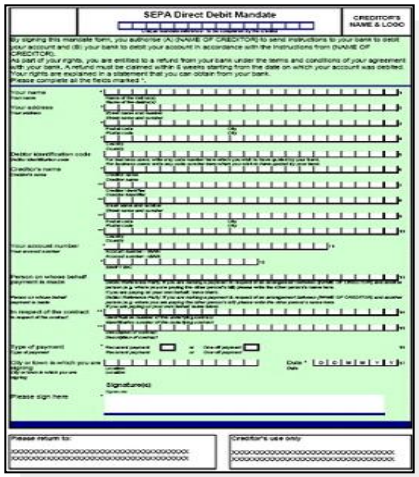
http://www.ecb.int/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf

2. CREATION OF THE SECURE PAY FORUM

Scope – Recommendations to improve the security of internet payments



Credit transfers



Direct debit
E-mandate

Payment cards

Virtual cards

Wallet solutions

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

Implementation

The recommendations should be implemented by PSPs and card payment schemes by 1 July 2014. National authorities may define shorter implementation periods.

The legal basis for implementation of the recommendations by the national authorities will be provided by the domestic legislation transposing the PSD and/or the existing oversight and supervisory competence of the relevant authorities.

→ Forum members shall support the implementation of the recommendations in their jurisdictions and strive to ensure effective and consistent implementation across jurisdictions

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

Focus on strong authentication – seen as a procedure that enables the PSP to verify the identity of a customer.

The use of two or more of the following elements is required:

- *something only the user knows, e.g. password, personal identification number;*
- *something only the user possesses, e.g. token, smart card, mobile phone;*
- *something the user is, e.g. biometric characteristic, such as a fingerprint.*

The elements selected must be mutually independent, at least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet.

The strong authentication procedure should be designed to mitigate the risks related to the confidentiality of the authentication data.

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

General control and security environment

I. Governance
II. Risk identification and assessment
III. Monitoring and reporting
IV. Risk control and mitigation
V. Traceability

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

I. Governance

PSPs should implement and regularly review a formal internet payment services security policy

KC *The PSP's security objectives and risk appetite should be defined in a internet payment services security policy .*

- → *documented, regularly reviewed and approved by senior management.*

KC *The policy should define roles and responsibilities,*

- → *including an independent risk management function,*
- → *reporting lines for internet payment services*
- → *management of sensitive payment data with regard to the risk assessment, control and mitigation.*

BP *The internet payment services security policy could be laid down in a dedicated document.*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

II. Risk identification and assessment

PSPs should regularly carry out and document thorough risk identification and vulnerability assessments with regard to internet payment services

KC *Risk identification and comprehensive vulnerability assessments of services the PSP offers or plans to offer (incl. outsourcing)*

KC *Determine necessary changes to the existing security measures, the technologies used and the procedures or services offered incl. implementation time and interim measures.*

KC *Address the need to protect and secure sensitive payment data, incl. the customer's and the PSP's credentials, and other information.*

KC *Review of the PSP's risk scenarios and security measures*
→ *after major incidents, before a major change & at least 1x p.a. general review*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

III. Monitoring and reporting

PSPs should ensure the central monitoring, handling and follow-up of security incidents, including security-related customer complaints. PSPs should establish a procedure for reporting such incidents to management and, in the event of major incidents, the competent authorities

KC *Process to centrally monitor, handle and follow up on security incidents/related customer complaints and report to management.*

KC *PSPs and CPS's procedure for notifying the competent authorities immediately in the event of major incidents*

KC *PSPs and CPS's procedure for cooperation on all data breaches with the relevant law enforcement agencies.*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

IV. Risk control and mitigation

PSPs should implement security measures in line with their internet payment services security policy in order to mitigate identified risks. These measures should incorporate multiple layers of security defences, where the failure of one line of defence is caught by the next line of defence ("defence in depth")

KC *Design, development and maintenance of internet payment services:*

- → *Adequate segregation of duties in IT environments;*
- → *"Least privileged" principle for identity and access management.*

KC *Limit their vulnerability of public websites and backend servers.*

- → *Use of firewalls, proxy servers etc. to protect networks, websites, servers and communication links against attackers or abuses*
- → *Strip the servers of superfluous functions*
- → *Strict restriction of access by applications to the data and resources required*
- → *Use of extended validation certificates or similar to enable customers to check the website's authenticity.*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

IV. Risk control and mitigation (cont)

KC *PSP's processes in place to monitor, track and restrict access to i) sensitive data, and ii) logical and physical critical resources.*

→ *create, store and analyse appropriate logs and audit trails.*

KC *Testing of security measures by the risk management function*

→ *Prior any changes to the service are put into operation.*

→ *Regular repetition of tests and including scenarios of potential attacks.*

KC *Periodical audits of the PSP's security measures by trusted and independent experts.*

KC *Compliance requirements in outsourcing contracts*

KC *Acquirers should require e-merchants to implement security measures on their website as described in this recommendation.*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

V. Traceability

PSPs should have processes in place ensuring that all transactions can be appropriately traced

KC *PSP security mechanisms for the detailed logging of transaction data*

- → *transaction sequential number, timestamps, parameterisation changes and access to transaction data*
- → *Tracing of any addition, change or deletion of transaction data*

KC *Querying and analysing the transaction data by the PSPs*

- → *special tools for evaluating log files; analysis only by authorised personnel*

BP *[cards] It is desirable that acquirers require e-merchants who store payment information to have these processes in place*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

Specific control and security measures for internet payments

VI. Initial customer identification, information

VII. Strong customer authentication

VIII. Enrolment and provision of strong authentication tools

IX. Log-in attempts, session time-out, validity of authentication

X. Transaction monitoring and authorisation

XI. Protection of sensitive payment data

XII. Customer education and communication

XIII. Notifications, setting of limits

XIV. Verification of payment execution by the customer

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

VI. Initial customer identification, information

Customers should be properly identified and confirm their willingness to conduct internet payment transactions before being granted access to such services. PSPs should provide adequate "prior" and "regular" information to the customer about the necessary requirements (e.g. equipment, procedures) for performing secure internet payment transactions and the inherent risks

KC *Customer identification and information prior granting access to the services.*

KC *Prior information supplied to the customer should include:*

- → *any requirements in terms of customer equipment, software or other tools*
- → *secure use of personalised security credentials or provided hard-/ software*
- → *description of the procedure to submit and authorise a payment, responsibilities and liabilities of the PSP and the customer*
- → *procedures in the event of loss /theft of the personalised security credentials or the customer's hardware or software for logging in or carrying out transactions*
- → *the procedures to follow if an abuse is detected or suspected*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

VI. Initial customer identification, information (cont)

KC *PSPs should ensure that the framework contract with the customer includes compliance-related clauses*

- → *prevention of money laundering*
- → *blocking of transactions on the basis of security concerns*
- → *method and terms of the customer notification and "unblocking"*

KC *Ongoing and appropriate provision of customers with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service*

BP *Dedicated rather than general service contract for internet payments*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

VII. Strong customer authentication

Internet payment services should be initiated by strong customer authentication

KC *[CT/e-mandate] Credit transfers (incl. batch CT) or electronic DD mandates should be initiated by strong customer authentication*

- → *Exemption for payments to trusted beneficiaries included in "white lists"*

KC *Access to or amending sensitive payment data requires strong authentication*

- → *Exemption on the basis of a risk analysis for purely consultative services, with no display of sensitive customer or payment information*

KC *[cards] Issuers should support strong cardholder authentication*

- → *All cards issued must be technically ready to be used with strong authentication*
- → *Prior consent of the cardholder to participating in such services.*

KC *[cards] Acquirers should support technologies allowing the issuer to perform strong cardholder authentication*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

VII. Strong customer authentication (cont)

KC *[cards] Acquirers should require their e-merchant to support strong authentication*

→ *Justification of exemptions by a (regularly reviewed) fraud risk analysis, with CVx2 as minimum requirement*

KC *[cards] CPSs should promote the implementation of strong customer authentication by introducing liability shifts in and across all European markets*

KC *[cards] Providers of wallet solutions should support technologies allowing the issuer to perform strong authentication when the legitimate holder first registers the card data and when executing transactions.*

→ *Justification of exemptions by a (regularly reviewed) fraud risk analysis, again with CVx2 as minimum requirement*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

VII. Strong customer authentication (cont)

KC *[cards] For virtual cards, the initial registration should take place in a safe and trusted environment. Strong authentication should be required for the virtual card data generation process if the card is issued in the internet environment.*

BP *[cards] Support of strong authentication of the cardholder by e-merchants.*

→ *Exemptions: the use of CVx2 is recommended*

BP *PSPs could consider using one authentication tool for all internet payment services*

→ *customer acceptance & proper use*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

VIII. Enrolment and provision of strong authentication tools

PSPs should ensure that customer enrolment for and the initial provision of strong authentication tools required to use the internet payment service is carried out in a secure manner

KC *Requirements for enrolment and provision of strong authentication tools:*

- → *The related procedures should be carried out in a safe and trusted environment (e.g. face-to-face, via an internet banking or other secure website, ATM)*
- → *Secure delivery of personalised security credentials and all internet payment-related devices and software*
  - *Physical distribution: sent by post or delivered with acknowledgement of receipt Software: digitally signed by the PSP*
  - *No distribution of credentials via e-mail or website.*
- → *[cards] The customer should have the option to register for strong authentication independently of a specific internet purchase. In addition, activation during online shopping could be offered by re-directing the customer to a safe and trusted environment (see above)*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

VIII. Enrolment and provision of strong authentication tools (cont)

KC *[cards] Issuers should actively encourage cardholder enrolment for strong authentication.*

- → *Cardholders should only be able to bypass strong authentication in exceptional cases where this can be justified by the risk related to the card transaction.*
- → *In case of exemptions cardholder name, personal account number, expiration date, CVx2 and/or static password should be a minimum requirement*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

IX. Log-in attempts, session time-out, validity of authentication

PSPs should limit the number of authentication attempts, define rules for payment session "time out" and set time limits for the validity of authentication

KC *The validity period of one-time password should be limited to the strict minimum necessary (i.e. a few minutes)*

KC *Maximum number of failed log-in or authentication attempts after which access to the internet service is (temporarily or permanently) blocked & secure procedure to re-activate blocked internet services*

KC *Automatic termination of inactive payment sessions after a maximum period*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

X. Transaction monitoring and authorisation

Security monitoring and transaction authorisation mechanisms aimed at preventing, detecting and blocking fraudulent payment transactions before they are executed should be conducted in real time; suspicious or high risk transactions should be subject to a specific screening and evaluation procedure prior to execution

KC *Real-time fraud detection and prevention systems to identify suspicious transactions*

- → *parameterised rules (such as black lists of compromised or stolen card data)*
- → *abnormal behaviour patterns of the customer /customer's access device (change of IP address /range during the internet payment session, geolocation IP checks, abnormal transaction data or e-merchant categories, etc.)*

KC *CPSs in cooperation with acquirers should elaborate a harmonised definition of e-merchant categories and require integration in the authorisation message*

BP *Appropriate time frame for screening and evaluation procedures by the PSP*

BP *PSPs notification of the customer of a blocking of a payment transaction; maintenance of the block for as short a period as possible.*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

XI. Protection of sensitive payment data

Sensitive payment data should be protected when stored, processed or transmitted

KC *All data or files used to identify and authenticate customers as well as the customer interface, should be appropriately secured against theft and unauthorised access or modification*

KC *When transmitting sensitive payment data, a secure end-to-end communication channel should be maintained throughout the entire duration of the internet payment service provided;*

→ *Use of strong and widely recognised encryption techniques*

KC *[cards] Acquirers should encourage e-merchants not to store any sensitive card payment data. In the event e-merchants handle, i.e. store, process or transmit sensitive data related to card payments he should be required to have the necessary measures in place to protect these data. PSPs should refrain from providing services to e-merchants who cannot ensure such protection*

BP *[cards] It is desirable that e-merchants handling sensitive cardholder data appropriately train their fraud management staff and update this training regularly*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

XII. Customer education and communication

PSPs should communicate with their customers in such a way as to reassure them of the integrity and authenticity of the messages received. The PSP should provide assistance and guidance to customers with regard to the secure use of the internet payment service

KC *Provision of a secured channel for ongoing customer communication regarding the correct and secure use of the internet payment service and explain:*

- → *that any message in this respect on behalf of the PSP via any other means, such as e-mail is not reliable.*
- → *the procedure for customers to report (suspected) fraudulent payments, suspicious incidents or anomalies during the internet payment session and/or possible social engineering attempts*
- → *how the PSP will respond to the customer*
- → *how the PSP will notify the customer about (potential) fraudulent transactions or warn the customer about the occurrence of attacks (e.g. phishing e-mails)*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

XII. Customer education and communication (cont)

KC *Through the designated channel, PSPs should keep customers informed about updates in procedures and security measures and provide alerts about significant emerging risks (e.g. warnings about social engineering)*

KC *Customers should be appropriately informed about how and where customer assistance regarding internet payments can be obtained.*

- → *questions, complaints, support and notifications of anomalies or incidents*

KC *PSPs and CPSs should initiate customer education and awareness programmes on:*

- → *Protection of passwords, security tokens, personal details & confidential data;*
- → *Proper management of the security of the personal device through installing and updating security components (antivirus, firewalls, security patches);*
- → *Threats and risks related to downloading software via the internet;*
- → *How to use the genuine internet payment website.*

BP *[cards] It is desirable that acquirers arrange educational programmes for e-merchants on fraud prevention.*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

XIII. Notifications, setting of limits

PSPs should provide their customers with options for risk limitation when using internet payment services. They may also provide alert services.

KC *Prior to providing internet payment services, PSPs should agree with each customer on spending limits applying to those services, or allow the customer to disable the internet payment functionality.*

BP *Customer facility to manage limits for internet payment services in a secure environment.*

BP *Alerts for customers, such as via phone calls or SMS*

BP *Enable customers to specify general, personalised rules as parameters for their behaviour with regard to internet payments*

→ *e.g. that they will only initiate payments from certain specific countries and that payments initiated from elsewhere should be blocked.*

3. RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

XIV. Verification of payment execution by the customer

PSPs should provide customers in good time with the information necessary to check that a payment transaction has been correctly executed

KC *PSPs should provide customers with a facility to check transactions and account balances at any time in a secure environment.*

KC *Any detailed electronic statements should be made available in a secure environment. Where PSPs inform customers through an alternative channel, such as SMS, e-mail or letter about the availability of electronic statements (e.g. monthly or ad hoc), sensitive payment data should not be included or, if included, they should be masked*

4. MAIN FOCUS & OUTLOOK

4. MAIN FOCUS & OUTLOOK

All interested parties are invited to comment on the draft "Recommendations for the security of internet payments" by 20 June 2012.

The document can be downloaded from the ECB's website.

Comments on the public consultation should be submitted to the ECB in English, or in the relevant official EU language, at the following address:

European Central Bank
Secretariat Division
Kaiserstrasse 29
D-60311 Frankfurt am Main, Germany
Fax: +49 69 1344 6170
E-mail: ecb.secretariat@ecb.europa.eu

4. MAIN FOCUS & OUTLOOK

- Public consultation until 20 June 2012
- Review of the recommendations by SecuRe Pay until end of 2012
- Integration of the recommendation in the supervisory and oversight expectations

SecuRe Pay work items for 2012

- Access to payment accounts over the internet by third party providers
- Mobile payments and NFC
- Information sharing on security incidents

QUESTIONS

THANK YOU

RUI PIMENTEL
Head of the Payment Systems Analysis and Development Unit
Payment Systems Department
Banco de Portugal
+351.21.3130944
rpimentel@bportugal.pt