FEDERATION
BANCAIRE
FRANCAISE

Response of the FBF to ECB Recommendations for the security of internet payments

Contributor	Fédération Bancaire Française 18 rue La Fayette 75440 Paris Cedex 08
Contact	Catherine Bertrand Tél : +33148005176 email: cbertrand@fbf.fr
Response Date	20 june 2012

I. GENERAL COMMENTS ON THE WHOLE DOCUMENT

On the one hand, the French Banking Federation (FBF) welcomes the effort made by the European Central Bank (ECB) to build a homogeneous and global security framework for internet payments, including all types of payment solutions in Europe.

On the other hand, the FBF would like to highlight the risk that the Forum recommendations which will be implemented by national authorities, could create distortions of competition from one country to another, or from a payment solution to another. Indeed, as detailed in our response, some players involved in the internet payment chain are not addressed by the report. Moreover, the way the recommendations are implemented will depend on the specific prerogatives of each competent national authority: this situation cannot guarantee a level playing field between payment service providers neither ensure an harmonization of practices, which is however one of the purposes of the Forum mandate[1] approved by the Governing Council.

Last but not least, by securing only one part of the payment chain on internet, there is a strong risk to have fraud focused on the weakest one.

A. General comments about the scope of those recommendations

- **Concerning the European field**

Some recommendations[2] from the Forum may not necessarily apply to non-European players who usually include the cost of risk in their business model. This situation could be detrimental to a level playing field for internet payments due to differentiated security requirements.
There is definitely a strong need to improve and harmonize European law and procedures in respect of all domains related to payment on internet, such as rules on security measures, cybercrime, data protection, anti-money laundering, etc. , so that liabilities and responsibilities, as defined in the corresponding legislation, are consistent with and reflect internet payment security requirements.

- **Concerning the use of all means of payment**

In many instances, the document seems to make the assumption that e-payment are always related to card payments. However other payment instruments may be used to pay e-merchants over the internet. It is considered that many statements of the report may be valid for other payment instruments when used over the internet.

Furthermore, because fraud has become multi-channel, it is essential to secure all channels involved in internet payment. That is the reason why some recommendations should also be applied to payment initiated by mail order or phone order, two channels that have to be added to the scope of the report.

In order not to create distortions of competition, the scope should be completed with the following issues:

- Credit transfer and direct debit transactions not using web-based technology
- e-banking operations made with corporate cards
- Card transactions for provisioning an e-money account (e.g. paypal)

---

[1] See Decisions taken by the Governing Council of the ECB
http://www.ecb.int/press/govcdec/otherdec/2011/html/gc110520.en.html

[2] Recommendations such as real time controls, detection of maximum number of transactions in a timeframe or strong authentications required regardless of maximum amounts

- **Concerning all players involved in the e-payment chain**

The document specifies recommendations to be followed by PSPs governed by the PSD. However with internet payments, there are many other players offering services without being subject to this legal framework. Since security of a (payment) system is as strong as its weakest point, this appears to be a missed chance. That is the reason why the security rules should apply and be enforced in the same way all over Europe to every actor involved in the payment chain, i.e. PSPs, e-merchants, consumers, non-regulated service providers, etc.

In addition, the French Banking Federation recalls that card payments schemes are also very much impacted by this report.

To conclude on that scope's subject, it needs to be added to the report that all exclusions listed will be subsequently treated.

- **Concerning the measures for securing the payments**

First of all, it appears necessary to clearly identify the compulsory aspect of Key Recommendation and Best Practice, regarding the risk analysis.

In some cases, the report goes into too much detail. As a consequence, the recommendations could become either inappropriate to some contexts or obsolete as a result of innovation. It has become a first priority to develop and implement evolved technical solutions. Therefore, the recommendations should be restricted to technology independent security requirements and avoid prescribing any specific technical solutions. In addition, contractual or technical obligations should be defined by the parties according to an adequate risk analysis undertaken on a case by case basis. Security credentials, passwords management, fraud detections, end sessions could be taken into consideration.

Moreover, if the document focuses merely on authentication aspects, thereby totally ignoring the security of the payment transaction and the linkage of the consumer authentication to the securing of the payment transaction, it has to be mentioned in the report, as part of a competitive space, this could not be more than good practices on this topic.

Last but not least, throughout the document there seems to be a mix up between risk management and audit functions/processes which should be better clarified. ISO/IEC 2700x series could provide some guidance to the editors.

As a result, the following sentence has to be added to the general part of the report : **"In Europe, the use of all means of payment has to be secured at the same level whatever the PSP involved."**

B. General comments about the legal aspects of those recommendations

The French Banking Federation underlines that the content of this report is not clear and its consequences are larger than expected, as dealing with items that are not directly related to security but are in the scope of :

- Data Protection Directive (e.g. Recommendation 11 on Protection on sensitive payments data, KC 3.2 organizing a notification to data protection authorities, KC 4.3 on processes related to sensitive data)
- Payment Services Directive (Recommendations 6, 12, 13 and 14 on information to be provided to consumers after payment execution)

These two directives are currently in an official process of revision (proposal of regulation of the Commission to review the Data Protection Directive; expected report of the Commission on the implementation and impact of the Payment Services Directive).

In addition, as previously mentioned, e-merchants and consumers should be involved in order to ensure the full control and security of the payment process; this would imply to update respectively the Directive 2000/31 on electronic commerce and the PSD.

Last but not least, some recommendations cover also the scope of industry based rules as well as the card schemes rules.

As a result, all this creates a lack of legal security concerning the implementation and control of these recommendations.

C. General comments about the recommendations implementation

The BCE recommendations are not enforceable by law. They will have to be integrated in local laws or within the EU to be implemented.
The French Banking Federation has understood that national authorities will be in charge of the implementation within all European Union, but wonders what detailed procedures the PSP would have to follow.
Moreover, some of the technical recommendations are part of the payment security framework and could certainly be integrated in France. However, other recommendations from part 6, 12, 13 and 14 could fall within the scope of the PSD, as already mentioned. The PSD is a full harmonization directive and therefore, exception aside, prevents any States members to enrol in more binding measures. It seems therefore necessary that the decision on whether to implement or not those recommendations should be taken at the European Union level (I.e. during the PSD revision process).
In France, will there be cooperation between the data protection authority (CNIL), the Autorité de Contrôle Prudentiel and la Banque de France, since these three authorities are very much concerned with the recommendations implementation?

In addition, the implementation of the report requires the identification of the instances in charge of controlling the compliance and punishing the non-compliance. Should such control be done by national regulators, a global reference framework is required to ensure harmonized control and sanction procedures all across Europe.

At least, the report specifies that the recommendations should be implemented by 1 July 2014. This timeframe does not appear to be a realistic objective since all the payment business lines (payment services, contractual aspects with customers and sub-contractors, information systems, PSP's procedures …) are involved. A new deadline should be fixed once the final report amended with the consultation results is ready.

II. GENERAL PART

	FBF Comments
1. Scope and addressees Excluded from the scope of the recommendations, key considerations and best practices are : 1) other internet services provided by a PSP via its payment website (e.g. e-brokerage, online contracts); 2) non-internet-based payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology; 3) transfers of electronic money between two e-money accounts; 4) credit transfers where a third-party accesses the customer's payment account; 5) redirections, i.e. where the payer is redirected to the PSP by a third party in the context of a credit transfer and/or direct debit, the redirection itself is excluded; 6) payment transactions made by an enterprise via dedicated networks; **7) card payments using corporate cards, i.e. cards issued to an enterprise for use by its employees or agents acting on its behalf;** **8) card payments using anonymous, nonrechargeable physical or virtual pre-paid cards where there is no ongoing relationship between the issuer and the virtual cardholder;** 9) the clearing and settlement of internet payment transactions, as this typically takes place via (designated) mechanisms other than the internet.	▪ Fraud has become multichannel ; therefore payments initiated by phone and mail have to be included in the scope of the report, as these two channels are more and more a fraudsters target. ▪ Why are items 7 and 8 related to specific types of cards excluded on page 5?
2. Guiding Principles First, PSPs should perform specific assessments of the risks associated with providing internet payment services, which should be regularly updated in line with the evolution of internet security threats and fraud. Some risks in this area have been identified in the past, for example by the Bank for International Settlements in 2003 6 or the Federal Financial Institutions Examination Council in 2005 and 2011.7. However, in view of the speed of technological advances and the introduction of new ways of effecting internet payments, along with the fact that fraudsters have become more organised and their attacks more sophisticated, a regular assessment of the relevant risks is of utmost importance. Second, as a general principle, the internet payment services provided by PSPs should be initiated by means of strong customer authentication. ***From the Forum's perspective, PSPs with no or only weak authentication procedures cannot, in the event of a disputed transaction, provide proof that the customer has authorised the transaction.***	▪ The 2nd principle is contradictory with the previous principle. The nature of authentication should be considered in the global context as a result of a risk analysis (maximum amount, maximum number of transactions in a timeframe, additional controls such as technical clues, checking for the terminal devices involved in the payment, global survey of the malevolent activity). Limiting things to strong authentication would disadvantage the European payment industry in the race with non-EC competitors. ▪ Concerning that paragraph: even if strong authentication contributes unquestionably to a reduction of fraud, it does not guarantee the fact that the user has allowed the transaction. The proof of that is nowadays malevolent software that practice man-in-the middle undercover transaction alteration.

	FBF Comments
Third, PSPs should implement effective processes for authorising transactions, as well as for monitoring transactions and systems in order to identify abnormal customer payment patterns and prevent fraud.	▪ This third principle confirms previous comments. We go toward transaction monitoring, transaction scoring because strong authentication is more and more circumvented.
3. Outline with the report The recommendations are organised into three categories. 1) General control and security environment of the platform supporting the internet payment service. As part of their risk management procedures, PSPs should evaluate the adequacy of their internal security controls against internal and external risk scenarios. Recommendations in the fi rst category address issues related to governance, risk identifi cation and assessment, monitoring and reporting, risk control and mitigation issues as well as traceability. 2) Specific control and security measures for internet payments. Recommendations in the second category cover all of the steps of payment transaction processing, from access to the service (customer information, enrolment, authentication solutions) to payment initiation, monitoring and authorisation. 3) Customer awareness, education and communication. Recommendations in the third category include customer protection, what customers are expected to do in the event of an unsolicited request for personalized security credentials, how to use internet payment services safely and, fi nally, how customers can check that the transaction has been executed	▪ We agree with those items.

III. RECOMMENDATIONS

A. General control and security environment

	FBF Comments
1. Governance PSPs should implement and regularly review a formal internet payment services security policy. **1.1 KC** The internet payment services security policy should be properly documented, and regularly reviewed and *approved by senior management*. It should define security objectives and the PSP's risk appetite. **1.2 KC** The internet payment services security policy should define roles and responsibilities, including an independent risk management function, and the reporting lines for internet payment services, including management of sensitive payment data with regard to the risk assessment, control and mitigation. **1.1 BP** The internet payment services security policy could be laid down in a dedicated document.	▪ **General comments**: Somewhere in this section on "General control & security environment" Business Continuity Plan and Incident Response team should be mentioned. ▪ **1.1 KC**: "*approved by senior management"* of whom? All parties involved should buy-in. ▪ The audit function should be separately identified in this section
2. Risk identification and assessment PSPs should regularly carry out and document thorough risk identification and vulnerability assessments with regard to internet payment services. **2.1 KC** PSPs, through their risk management function, should carry out and document detailed risk identification and vulnerability assessments, including the assessment and monitoring of security threats relating to the internet payment services the PSP offers or plans to offer, taking into account: i) the technology solutions used by the PSP, ii) its outsourced service providers and, iii) all relevant services offered to customers. PSPs should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines both on the side of the PSP[8] and *the customer*[9]. **2.2 KC** On this basis and depending on the nature and significance of the identified security threats, PSPs should determine whether and to what extent changes may be necessary to the existing security measures, the technologies used and the procedures or services offered. PSPs should take into account the time required to implement the changes (including customer roll-out) and take the appropriate interim measures to minimise disruption.	▪ **General comment:** Those recommendations are on line to act against certain practices yet criticized through the answers to the Green paper (KC 2.3 especially) ▪ **2.1 KC:** The complete environment should be taken into account as well in a risk assessment. The same rules must be applied to all the players of market (PSP, other service providers, e-retailers …) insofar as they make payment or store payment details. PSP have often subcontractors and cannot control the way this recommendation will be implemented by them. What definition of customer applies here: both consumers and e-merchants?

	FBF Comments
2.3 KC The assessment of risks should address the need to protect and secure sensitive payment data, including: i) both the customer's and the PSP's credentials used for internet payment services, and ii) any other information exchanged in the context of transactions conducted via the internet. **2.4 KC** PSPs should undertake a review of the risk scenarios and existing security measures both after major incidents and before a major change to the infrastructure or procedures. In addition, a general review should be carried out at least once a year. The results of the risk assessments and reviews should be submitted to senior management for approval.	▪ **2.3 KC**: Not only sensitive data should be secured, all payment transaction related data should be secured with respect to integrity and origin. 2.3 KC has to be amended as suggested: "The assessment of risks should address the need to protect and secure sensitive payment data, *transaction end-to-end data,* including: i) both the customer's and the PSP's credentials used for internet payment services, and ii) any other information exchanged in the context of transactions conducted via the internet."
3. 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. **3.1 KC** PSPs should have a process in place to centrally monitor, handle and follow up on security incidents and security-related customer complaints and report such incidents to the management. **3.2 KC** PSPs and card payment schemes should have a procedure for notifying the competent authorities (i.e. supervisory, oversight and data protection authorities) immediately in the event of major incidents with regard to the services provided. **3.3 KC** PSPs and card payment schemes should have a procedure for cooperating on all data breaches with the relevant law enforcement agencies.	▪ **General comments:** In France, those recommended processes are in place, reinforced by the support of all the CERT (Computer Emergency Response Teams). ▪ **Introductory paragraph:** Equally, the exchange of such information with other PSPs might in some cases be more than useful. ▪ **3.2 KC:** Establishing an incident notification procedure requires an agreement at European level on definition and qualification of incidents as well as notification delays. ▪ **3.3 KC:** Today this procedure exists for the most part. The cooperation of all card payment schemes is essential to ensure optimal performance of that reporting process.

	FBF Comments
4. 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"). **4.1 KC** In designing, developing and maintaining internet payment services, PSPs should pay special attention to the adequate segregation of duties in information technology (IT) environments (e.g. the development, test and production environments) and the proper implementation of the "least privileged" principle 10 as the basis for a sound identity and access management. **4.2** KC Public websites and backend servers should be secured in order to limit their vulnerability to attacks. PSPs should use firewalls, proxy servers or other similar security solutions that protect networks, websites, servers and communication links against attackers or abuses such as "man in the middle" and "man in the browser" attacks. PSPs should use security measures that strip the servers of all superfluous functions in order to protect (harden) and eliminate vulnerabilities of applications at risk. Access by the various applications to the data and resources required should be kept to a strict minimum following the "least privileged" principle**. In order to restrict the use of " fake" websites imitating legitimate PSP sites, transactional websites offering internet payment services should be identified by extended validation certificates drawn up in the PSP's name or by other similar authentication methods, thereby enabling customers to check the website's authenticity.**	▪ **General comments:** Security solutions implemented by PSP must answer to a risk analysis and not rules. ▪ **4.2 KC:** Firewalls and proxy servers are of no use against "man in the middle" and "man in the browser attacks". Letting think the contrary in a normative document is hazardous. Considering the last sentence of this paragraph (in bold), we do not think that customers have the technical skills to "check the website's authenticity". If the "extended validation certificates" or the "authentication methods" dedicated to customers are simple ones, the same methods will also be simple for fraudsters. If the same "certificates" or "authentication methods" are complex, customers will not be able to use them and there will be no more e-commerce transaction any more. The Eurosystem, which is responsible for the smooth functioning of payments, and the European Commission, which is responsible for consumer protection together with the Police organisations, should check the e-merchants websites and forbid and eliminate those that are fake. A "Central European Desk" located at the Eurosystem or at the European Commission in cooperation with the relevant European Police Organizations should be made available to European citizens so that they can inform the authorities when they think they have seen a fake e-merchant web site. In case of a fake e-merchant website, the latter authorities could then swiftly block or close the fake website. Moreover, since the customer cannot see whether an e-merchant website is within the European Union, these authorities should be able to check also e-merchant websites that are outside the European Union. Of course, this can only be done in cooperation with the authorities of the concerned countries that are outside the EU. As said in the second last paragraph of page 22 of Eurosystem's document, "cyber fraud is a global offence which needs a global and harmonised response".

	FBF Comments
4.3 KC PSPs should have processes in place to monitor, track and restrict access to: i) sensitive data, and ii) logical and physical critical resources, such as networks, systems, databases, security modules, etc. PSPs should create, store and analyse appropriate logs and audit trails. **4.4 KC** Security measures for internet payment services should be tested by the risk management function to ensure their robustness and effectiveness. Tests should also be performed before any changes to the service are put into operation. On the basis of the changes made and the security threats observed, tests should be repeated regularly and include scenarios of relevant and known potential attacks. **4.5 KC** The PSP's security measures for internet payment services should be periodically audited to ensure their robustness and effectiveness. The implementation and functioning of the internet services should also be audited. The frequency and focus of such audits should take into consideration, and be in proportion to, the security risks involved. Trusted and independent experts should carry out the audits. They should not be involved in any way in the development, implementation or operational management of the internet payment services provided. **4.6 KC** Whenever PSPs and card payment schemes outsource core functions related to the security of the internet payment services, the contract should include provisions requiring compliance with the principles and recommendations set out in this report. **4.7 KC** PSPs offering acquiring services should require e-merchants to implement security measures on their website as described in this recommendation.	▪ **4.3 KC:** Add to the end of the last line *" in these environments"* ▪ **4.4 KC**: Should the audit function not have a role in this rather than the risk management functions? ▪ **4.7 KC:** PSPs are not responsible for the security of their customers' merchant website. This recommendation would imply to update the Directive 2000/31 on electronic commerce. Therefore, this "Key Consideration" should be a "Best Practice" as made for paragraph *5 5.1 BP*. Indeed, the content of these provisions are discussed in each contractual relation between an e-merchant and each of its PSP in a competitive space. So, a "Best practice" should relate only to the existence of contractual clauses concerning the safety measures to apply by the e-retailer who enlists at a PSP.

	FBF Comments
5. Traceability PSPs should have processes in place ensuring that all transactions can be appropriately traced. **5.1 KC** PSPs should ensure that their service incorporates security mechanisms for the detailed logging of transaction data, including the transaction sequential number, timestamps for transaction data, parameterisation changes and access to transaction data. **5.2 KC** PSPs should implement log fi les allowing any addition, change or deletion of transaction data to be traced. **5.3 KC** PSPs should query and analyse the transaction data and ensure that any log fi les can be evaluated using special tools. The respective applications should only be available to authorised personnel. **5.1 BP [cards]** It is desirable that PSPs offering acquiring services require e-merchants who store payment information to have these processes in place.	▪ **General comments**: Those KC's are currently implemented.

B. SPECIFIC CONTROL AND SECURITY MEASURES FOR INTERNET PAYMENTS

	FBF Comments
6. 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. **6.1 KC** PSPs should ensure that the customer has undergone the necessary identification procedures and provided adequate identity documents and related information before being granted access to the internet payment services. **6.2 KC** PSPs should ensure that the prior information supplied to the customer contains specific details relating to the internet payment services. These should include, as appropriate : ▪ clear information on any requirements in terms of customer equipment, software or other necessary tools (e.g. antivirus software, firewalls); ▪ guidelines for the proper and secure use of personalised security credentials; ▪ a step-by-step description of the procedure for the customer to submit and authorise a payment, including the consequences of each action; ▪ guidelines for the proper and secure use of all hardware and software provided to the customer; ▪ the procedures to follow in the event of loss or 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; ▪ a description of the responsibilities and liabilities of the PSP and the customer respectively with regard to the use of the internet payment service. **6.3 KC** PSPs should ensure that the framework contract with the customer includes compliance-related clauses enabling the PSP to fulfil its legal obligations relating to the prevention of money laundering, which may require it to suspend execution of a customer's payment transaction pending the necessary regulatory checks and/or to refuse to execute it. The contract should also specify that the PSP may block a specific transaction or the payment instrument on the basis of security concerns. It should set out the method and terms of the customer notification and how the customer can contact the PSP to have the service "unblocked", in line with the Payment Services Directive. **6.4 KC** PSPs should also ensure that customers are provided, on an ongoing basis and via appropriate means (e.g. leaflets, website pages), with clear and straightforward instructions	▪ **6.2 KC:** Concerning the information given to the consumer, they are already listed within the PSD. So, should this recommendation be relevant, it should concern the PSD revision. However breaking down the payment script as proposed in this recommendation may complicate internet payments and neutralize all the effort developped at EU level, from the payment industry but also from the authorities to facilitate e-payment. So, regarding the information to be communicated, the security operating measures and the various steps of the payment process, a 'risk' approach is advisable as indicated by the European Commission within the Green Paper on card, mobile and internet payments (4.5:" the trade-off between security, speed and ease of use should be taken into account.") Going further than PSD requirements could have a contrary effect with the pursued goal: too many detailed information could worry them when using their means of payment, even encourage them to make unjustified complaints. Moreover, such situation could make things easily for the real fraudsters. Information must be concise, clear and understandable for everyone. PSP are not able to communicate about the hardware and software security that do not belong to them. Consumers are responsible for keeping their computer safe. In addition, warnings on social engineering attacks should be included in these recommendations. **Concerning the 6.2 KC last bullet :** It should be noted that a necessary harmonization is to be found at the European level in view of distortions appeared during the transpositions of the PSD. ▪ **6.3 KC :** This recommendation does not seem to belong to a document on security requirements (see paragraph I.B General

	FBF Comments
explaining their responsibilities regarding the secure use of the service. **6.1 BP** It is desirable that the customer signs a dedicated service contract for conducting internet payment transactions, rather than the terms being included in a broader general service contract with the PSP. **6.5 BP** It is desirable that the customer signs a dedicated service contract for conducting internet payment transactions, rather than the terms being included in a broader general service contract with the PSP.	comments about the legal aspects of those recommendations / Protection of sensitive data) In addition, as already mentioned in the previous comment, this recommendation goes too much into detail. ▪ **6.1 BP :** Whilst it is legitimate that internet payments be subject to contractual arrangements, individual institutions should be allowed to decide how they organize their contractual relationships with their customers.
7. Strong customer authentication Internet payment services should be initiated by strong customer authentication. **7.1 KC** [CT/e-mandate] Credit transfers (including bundled credit transfers) or electronic direct debit mandates should be initiated by strong customer authentication. PSPs could consider adopting less stringent customer authentication for outgoing payments to trusted beneficiaries included in previously established "white lists", i.e. a customer-created list of trusted counterparties and beneficiary accounts with strong authentication. **7.2 KC** Obtaining access to or amending sensitive payment data requires strong authentication. Where a PSP offers purely consultative services, with no display of sensitive customer or payment information, such as payment card data, that could be easily misused to commit fraud, the PSP may adapt its authentication requirements on the basis of its risk analysis. **7.3 KC [cards]** For card transactions, all PSPs offering issuing services should support strong authentication of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication (e.g. for 3-D Secure, registered in the 3-D Secure Directory) and the customer must have given prior consent to participating in such services. (See Annex 3 for a description of authentication under the cards environment.) **7.4 KC [cards]** All PSPs offering acquiring services should support technologies allowing the issuer to perform strong authentication of the cardholder for the card payment schemes in which the acquirer participates. **7.5 KC [cards]** PSPs offering acquiring services should require their e-merchant to support strong authentication of the cardholder by the issuer for card transactions via the internet. Exemptions to this approach should be justified by a (regularly reviewed) fraud risk analysis.	▪ These provisions are on line with the current recommendations of the French central Bank and implemented at the French banking community level as regards home banking and payment cards. ▪ PSPs could consider adopting less stringent customer authentication provided that it submits the appropriate risk analysis to the regulator. This implies harmonized rules and methods in order to ensure free competition between PSPs. This self-assessment method don't seem appropriate and the involvement of a Trusted third-party certified by a central and independent organization would have to be required. ▪ **7.1 KC :** As previously stated, the ability to initiate a transaction without strong authentication could be possible in consideration of several risk limiting factors (dynamic analysis of the characteristics of the transaction, limitation of amount, limits on the maximum number and amount of inbound payments a customer can receive, etc.). ▪ **7.1 et 7.2 KC :** The recommendations are contradictory. The word "purely" must be deleted in the 7.2 KC. ▪ **7.3 KC :** It does not seem necessary to ask the consumer to sign

	FBF Comments
In the case of exemptions, the use of the card verification code, CVx2, should be a minimum requirement. **7.6 KC [cards]** All card payment schemes should promote the implementation of strong customer authentication by introducing liability shifts (i.e. from the e-merchant to the issuer) in and across all European markets. **7.7 KC [cards]** For the card payment schemes accepted by the service, providers of wallet solutions should support technologies allowing the issuer to perform strong authentication when the legitimate holder first registers the card data. Providers of wallet solutions should support strong user authentication when executing card transactions via the internet. Exemptions to this approach should be justified by a (regularly reviewed) fraud risk analysis. In the case of exemptions, the use of CVx2 should be a minimum requirement. **7.8 KC [cards]** For virtual cards, the initial registration should take place in a safe and trusted environment (as defined in Recommendation 8). Strong authentication should be required for the virtual card data generation process if the card is issued in the internet environment. **7.1 BP [cards]** It is desirable that e-merchants support strong authentication of the cardholder by the issuer in card transactions via the internet. In the case of exemptions, the use of CVx2 is recommended. **7.2 BP** For customer convenience purposes, PSPs providing multiple payment services could consider using one authentication tool for all internet payment services. This could increase acceptance of the solution among customers and facilitate proper use.	an agreement, considering that he has already been informed about authentication methods he can use. Moreover, that would compel the PSPs to refuse all secured payments ordered by their costumers until they sign their agreement to make internet payments. This could create a situation in favor of non-secured payments. ▪ **7.5 KC :** The ECB suggests that PSPs offering acquiring services should require their e-merchant to support strong authentication of the cardholder by the issuer for card transactions via the internet. Because of the lack of an appropriate legal framework, this recommendation cannot be implemented. ▪ In addition, one must be aware that the CVx2 verification is a very weak protection against keyloggers, trodjans, etc... ▪ **7.7 KC :** Exemptions are allowed if fraud risk analysis. In this case, we agree. ▪ **7.5 KC et 7.7 KC :** There is also the matter of recurring payment for which neither strong authentication nor CVX2 can be used. This comment about the impossibility of using CVX2 is also relevant to eWallet solutions. ▪ **7.8 KC** : Payments made with e-cards are secured by the unique card number used for each transaction. Requiring strong authentication is not necessary in that case and would be detrimental to this type of product. ▪ **7.2 BP :** PSPs usually offer one authentication tool to consumers. But their different ways of paying may require several authentication tools, according to the nature of their transactions.

	FBF Comments
8. Enrolment for 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. **8.1 KC** Enrolment for and provision of strong authentication tools should fulfil the following requirements. The related procedures should be carried out in a safe and trusted environment (e.g. face-to-face at a PSP's premises, via an internet banking or other secure website offering comparable security features, or via an automated teller machine). Personalised security credentials and all internet payment-related devices and software enabling the customer to perform internet payments should be delivered securely. Where tools need to be physically distributed, they should be sent by post or delivered with acknowledgement of receipt signed by the customer. Software should also be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with. Moreover, personalised security credentials should not be communicated to the customer via e-mail or website. [cards] For card transactions, 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, preferably to an internet banking or other secure website offering comparable security features. **8.2 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 such instances, weak authentication based on the cardholder name, personal account number, expiration date, card verification code (CVx2) and/or static password should be a minimum requirement.	▪ PSPs are responsible for defining and implementing processes to enroll their customers for strong authentication services, based on their risks analysis. Therefore this recommendation appears to be too restrictive.

	FBF Comments
9. 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. **9.1 KC** When using a one-time password for authentication purposes, PSPs should ensure that the validity period of such passwords is limited to the strict minimum necessary (i.e. a few minutes). **9.2 KC** PSPs should set down the maximum number of failed log-in or authentication attempts after which access to the internet service is (temporarily or permanently) blocked. They should have a secure procedure in place to re-activate blocked internet services. **9.3 KC** PSPs should set down the maximum period after which inactive payment sessions are automatically terminated, e.g. after ten minutes.	▪ **9.3 KC**: This recommendation has to be amended as suggested: "PSPs should set down the maximum period after which inactive payment sessions are automatically terminated ***after a few minutes*****."**
10. Recommendation 10: 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. **10.1 KC** PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules (such as black lists of compromised or stolen card data), abnormal behaviour patterns of the customer or the customer's access device (change of Internet Protocol (IP) address12 or IP range during the internet payment session, sometimes identified by geolocation IP checks,13 abnormal transaction data or e-merchant categories, etc.) and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions should be commensurate with the outcome of the fraud risk assessment. **10.2 KC** Card payment schemes in cooperation with acquirers should elaborate a harmonised definition of e-merchant categories and require acquirers to implement it accordingly in the authorisation message conveyed to the issuer.14 **10.1 BP** It is desirable that PSPs perform the screening and evaluation procedure within an appropriate time period, in order not to unduly delay execution of the payment service concerned. **10.2 BP** It is desirable that PSPs notify the customer of the eventual blocking of a payment transaction, under the terms of the contract, and that the block is maintained for as short a period as possible until the security issues have been resolved.	▪ **General :** As regards complex and expensive means and process to implement the homogeneity of the practices and projects of the European banking world on the matter is to be checked ▪ **10.1 KC:** Being able to do that kind of real time analysis (and more) is desirable and should lower the need for strong authentication. Nevertheless, schemes and PSP must be responsible for that. ▪ Moreover, the question of the geolocation with the implementation of the IPV6 has to be re-examined in term of feasibility and potential earning as regards geolocation could be extremely complex to implement, and, in addition, could allow to mark the way for fraudulent people. Concerning the examples given in the document, it may appear quite dangerous to enter these security details. By mentioning them, we are likely to help fraudsters .It is therefore advisable to delete these examples.

	FBF Comments
11. Recommendation 11: Protection of sensitive payment data Sensitive payment data should be protected when stored, processed or transmitted. 11.1 KC All data or files used to identify and authenticate customers (at log-in and when initiating internet payments or other sensitive operations), as well as the customer interface (PSP or e-merchant website), should be appropriately secured against theft and unauthorised access or modification. 11.2 KC PSPs should ensure that when transmitting sensitive payment data, a secure end-to-end communication channel is maintained throughout the entire duration of the internet payment service provided in order to safeguard the confidentiality of the data, using strong and widely recognised encryption techniques. 11.3 KC [cards] PSPs offering acquiring services should encourage their e-merchants not to store any sensitive payment data related to card payments. In the event e-merchants handle, i.e. store, process or transmit sensitive data related to card payments, such PSPs should require the e-merchants to have the necessary measures in place to protect these data and should refrain from providing services to e-merchants who cannot ensure such protection. 11.1 BP [cards] It is desirable that e-merchants handling sensitive cardholder data appropriately train their dedicated fraud management staff and update this training regularly to ensure that the content remains relevant to a dynamic security environment.	▪ **General comments:** There is a recommendation missing on securing the integrity of the transaction/payment related data and its origin. ▪ **KC 11.3:** It must be recalled that the customers are the ones who communicate "sensitive datas" to the e-merchants and not the PSPs. The customers should thus be responsible to require that the e-merchants have the "necessary measures in place". But, since the customers do not have the technical skills to require and to check this with the e-merchants, the e-merchants who are storing, processing or transmitting sensitive data should be granted a license by an authority so that they can be supervised by it. This would be the only credible way to make these requirements and to check if the requirements are fulfilled. It must be recalled that in case there is a theft of sensitive data, the fraudsters can use them to initiate payments. It must here also be recalled that "acquirers" in Europe are not always PSPs and are thus not always covered by the PSD. Non-PSP acquirers are not all supervised today. Acquirers should also be covered by the PSD and be supervised by the appropriate national authority. ▪ **BP 11.1:** This provision would deserve to see e-merchants who store sensitive data, be integrated in the scope of the the regulation and be assigned a regulated specific status to be defined in the forthcoming update of the PSD. If no regulatory status exists, this recommendation would remain a "wishful thinking".

C. Customer awareness, education and communication

	FBF Comments
12. 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. **12.1 KC** PSPs should provide at least one secured channel 15 for ongoing communication with customers regarding the correct and secure use of the internet payment service. PSPs should inform customers of this channel and explain that any message on behalf of the PSP via any other means, such as e-mail, which concerns the correct and secure use of the internet payment service, is not reliable. The PSP should explain: ▪ the procedure for customers to report to the PSP (suspected) fraudulent payments, suspicious incidents or anomalies during the internet payment session and/or possible social engineering 16 attempts; ▪ the next steps, i.e. 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). **12.2 KC** Through the designated channel, PSPs should keep customers informed about updates in procedures and security measures regarding internet payment services. Any alerts about significant emerging risks (e.g. warnings about social engineering) should also be provided via the designated channel. **12.3 KC** Customer assistance should be made available by PSPs for all questions, complaints, requests for support and notifications of anomalies or incidents regarding internet payments, and customers should be appropriately informed about how such assistance can be obtained. **12.4 KC** PSPs and, where relevant, card payment schemes should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need: ▪ to protect their passwords, security tokens, personal details and other confidential data; ▪ to manage properly the security of the personal device (e.g. computer), through installing and updating security components (antivirus, firewalls, security patches); ▪ to consider the significant threats and risks related to downloading software via the internet if the customer cannot be reasonably sure that the software is genuine and has not been tampered with; ▪ to use the genuine internet payment website. **12.1 BP [cards]** It is desirable that PSPs offering acquiring services arrange educational programmes for their e-merchants on fraud prevention.	▪ **12.4 KC 1st bullet sentence :** Add « and not share it with any other third party »

	FBF Comments
13. Recommendation 13: 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. **13.1 KC** Prior to providing internet payment services, PSPs should agree with each customer on spending limits applying to those services. (e.g. setting a maximum amount for each individual payment or a cumulative amount over a certain period of time), and on allowing the customer to disable the internet payment functionality. **13.1 BP** Within the agreed limits, e.g. taking into account overall spending limits on an account, PSPs could provide their customers with the facility to manage limits for internet payment services in a secure environment. **13.2 BP** PSPs could implement alerts for customers, such as via phone calls or SMS, for fraud-sensitive payments based on their risk-management policies. **13.3 BP** PSPs could 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.	▪ **13.1 KC and 13.1 BP**: Due to the existing legal framework, the consumer is already informed about the way of using his means of payment offered by his PSP, including their spending limits. Furthermore payment on the internet is one of the channels to order a payment and not a mean of payment as such. In some situation it even might be multi-channel. As a consequence, these two items must be deleted from the report : ▪ 13.3 BP: 13.3 must also be deleted as the measure is no longer appropriate to the way Internet evolves regardless of geographic borders. There is also a risk to have this measure corrupted by fraudsters.
14. Recommendation 14: 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. **14.1 KC** PSPs should provide customers with a facility to check transactions and account balances at any time in a secure environment. **14.2 KC** Any detailed electronic statements should be made available in a secure environment. Where PSPs periodically inform customers about the availability of electronic statements (e.g. when a new monthly e-statement has been issued, or on an ad hoc basis after execution of a transaction) through an alternative channel, such as SMS, e-mail or letter, sensitive payment data should not be included in such statements or, if included, they should be masked.	▪ **14.1 KC:** The provisions listed in recommendation 14 are already in place for a long time in France. ▪ **14.2 KC:** The recommendation has to be redrafted without mentioning “e-mail” as part of the alternative channel list. In addition, it should be specify that e-mails must be avoided to inform customers as phishing attacks are also based on that mean of communication.

D. Annex

	FBF Comments
▪ Glossary of terms ▪ Annex 1: the review of the payment services directive: points to consider ▪ Annex 2: security of the environment underpinning internet payments ▪ Annex 3: architecture for cardholder authentication via the internet ▪ Annex 4: list of authorities participating in the work of the european forum on the security of retail payments	▪ **Glossary**: Define: consumer, customer, e-merchant, payment scheme. All definition should be consistent with those used in the PSD. ▪ **Annex II - Points 1 & 2 :** These points are mentioning ""MIE, Firefox, Google Chrome, Opera, Safari … Microsoft, Mozilla …Verisign, Entrust, Comodo, Global sign … RSA, Vasco". It may be inappropriate to mention these details in a public report as it may lead to a restriction in the solutions to be used and increase the risk of massive fraud. By mentioning these details, does the Eurosystem not help the fraudsters? It is probably better not to mention these details.