Author: Úna Dillon, Irish Payment Services Organisation (IPSO) 18th June 2012

ECB Recommendations for the Security of Internet Payments

Response from the Irish Payment Services Organisation (IPSO) in consultation with IPSO members

1 GENERAL PART – COMMENTS:

IPSO welcomes this paper which provides recommendations and best practices to the payments industry for the prevention of internet payment fraud. We also welcome the opportunity to comment on the paper and provide our remarks below, for consideration by the ECB.

While IPSO agrees in principle to all of the recommendations we have a number of specific concerns which we would like to raise; namely:

1. In the main, the paper aims "to foster the establishment of a harmonised EU / EEA wide minimum level of security". While we support this suggestion we have a concern that the harmonisation of security measures for internet payments is not entirely effective when focussed on a specific geographical area.

   In the general part of the paper the ECB itself states that "the safety of internet payments depends on the responsible behaviour of all actors". We agree completely with this statement, however "all actors" includes many e-retailers and PSPs outside of the EU / EEA region.

   While security measures can be and are implemented in the EU / EEA market, there is a need to engage more forcefully with industry standard makers and authorities in other jurisdictions otherwise the paper, while promoting security in a 'level playing field', does not actually cover the whole 'field', as it were.

   IPSO is not content with the exclusion of some key actors in the payments landscape from the more rigorous approach to security recommended here. In particular the exclusion of e-money providers has the potential to result in an explosion of low value fraud through this mechanism. Two levels of recommendations might be more all-encompassing and avoid an unregulated, lower tier of payments developing.

   On a similar note, the paper refers to it applying only to those institutions which are covered under the PSD. We would suggest that it should apply to all stakeholders and parties involved in the internet payment transaction process, to avoid any weak links which prevent the recommended security measures from being effective.

2. With regard to the timelines for the implementation of the recommendations we suggest that the period in question, i.e. to 1st July 2014, is too aggressive. The short timeframe does not allow for appropriate research of relevant security tools that might be available to the market, or

engagement with the parties which provide those tools.

There is also a risk that the tight timeline will lead to current plans for innovation in payments to be postponed while PSPs focus on the implementation of new security measures; which, we would add, are not necessarily proven to prevent internet fraud.

With regard to 2-factor authentication, we have no issue in principle but would like to point out the challenge this creates for implementation in certain remote payment circumstances (e.g. Card Not Present). This is not to suggest that it should not be implemented but that a July 2014 deadline may be difficult to achieve for this payment method.

In the context of the recommendations regarding security measures, we would suggest that there should be industry-wide / European solutions available to *all* parties. We would suggest that the production of such solutions will require consultation, research, input from industry stakeholders and experts, investment and vendors willing to produce the required software and hardware. This process will take longer than the required two years.

Timeframe: July 2014 – we believe the extent of the recommendations is wide-ranging. A phased and 'rolling' approach would better achieve the desired outcome. The paper itself observes the need for on-going governance and review. Setting a challenging end date is not necessarily consistent with this approach. For example, an on-going 18-month review cycle with a progressive uplift of the minimum standards required would provide an achievable and on-going framework within which to operate.

3. Exclusions: With regard to the exclusions, we would ask why the transfer of e-money between two e-money accounts would be omitted. We would suggest that this is a key area of concern, especially where cardholder accounts are infiltrated through Phishing scams, etc. and money transferred from those accounts without the cardholder's authority to a criminal's account (which itself is normally established through fraudulent means, etc.).

   We also question the exclusion of card payments made using corporate cards. These transactions are open to the same risks as all other payment cards, when used on the internet.

4. Regarding the implementation of 'strong cardholder authentication', we agree with the concept however we would have a concern that strong tools for cardholder authentication are lacking in the market. We believe that the ECB should put an emphasis on the need for card schemes to support their members' fraud prevention activities. The existing tools have been available in the market for some time, and while retail banks have implemented additional fraud prevention methods in their systems, organised crime has become more sophisticated and continues to evolve; quicker than the industry can react.

5. We believe that responsibility for the recommendations should be clarified, e.g. for some points it is not clear if the card schemes, card issuers or retail banks have responsibility for their implementation.

6. In the context of national bodies overseeing the implementation of the recommendations, IPSO supports the view that the recommendations be provided with minimum standards outlined (for security, protocols, etc.). Regulation on such security measures could potentially lead to difficulties for new players joining the internet payments market while the costs of implementing potentially out-dated security measures would be too great for new players to the market.

   We believe there should be a set of minimum security standards produced out of this consultation

process, for implementation by all stakeholders.

7. IPSO supports the recommendation that acquiring services should only be provided by licensed providers.

8. IPSO recognises the use of a fraud liability shift as a means to encourage e-merchants to implement strong authentication methods. We would like to note however that consumers' convenience must not be neglected.

9. Engagement with law enforcement: We suggest to the ECB that it considers the requirement for PSPs to engage with law enforcement. This type of engagement is not hugely referred to in the recommendations, while it is an important tool for crime prevention.

   All parties in the EU / EEA should be encouraged to develop such a liaison. In a similar context, there should be more engagement between law enforcement agencies and industry fraud prevention groups across the EU / EEA.

10. In the context of internet card payments, we believe that the industry's Payment Card Industry Data Security Standards (PCI DSS), with which all card issuers and acquirers must comply, address the issue of protection of sensitive information such as cardholder data.

    It should be noted however that while the card issuers and acquirers can implement security measures in this regard, there is a dependency on the cardholder to also ensure the security of their internet shopping environment.

    The ECB should consider that not all of the protection available is controllable by the banks and that cardholders need to take responsibility also.

11. Appropriate mix of security elements: We suggest that the focus should be on the outcomes required rather than being too prescriptive about the methods used to achieve same. This will facilitate continuation of competition in this area (through innovation around security) while avoiding unnecessary 'double spend' on multiple security features which achieve the same end.

12. Stakeholder: We recognise the need to engage all actors in the value chain. While the onus can sit with the larger, more 'institutional players' it recognises the need to engage, educate and communicate to all actors in the value chain.

Our further comments on each recommendation are below.

RECOMMENDATIONS

GENERAL CONTROL AND SECURITY ENVIRONMENT

Recommendation 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.*

RECOMMENDATION 1 – COMMENT:

We agree with this recommendation. This policy should be implemented as a matter of principle and it is reassuring that the ECB is making such a recommendation to all parties.

Recommendation 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.*

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.*

RECOMMENDATION 2 – COMMENT:

We agree with this recommendation.

Recommendation 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.*

RECOMMENDATION 3 – COMMENT:

IPSO agrees with this recommendation.

Recommendation 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.*
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.*

RECOMMENDATION 4 – COMMENT:

4.2 KC: It should be noted that with respect to "man in the browser attacks" there is currently no known solution available to the industry to guarantee protection. As such, while we agree that PSPs should protect against this type of attack, the solutions are not always available, thus making full protection impossible.

In terms of "extended validation certificates" (EVCs), our view is that these offer limited value from a security perspective. Their main value is related to customer education and there are many examples of user behaviour which prove that the bank cannot count on every customer's awareness of the risks.

Furthermore, EVCs do not prevent against the growing number of attacks where malware modifies what the customer sees in the browser e.g. 'Man in the Browser' attacks where rogue software on a customer's computer dupes the customer into believing they are on a genuine site and facilitates their inadvertent processing of payments to the criminal's account.

Recommendation 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 files 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 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.*

RECOMMENDATION 5 – COMMENT:

We have no issues with this recommendation.

SPECIFIC CONTROL AND SECURITY MEASURES FOR INTERNET PAYMENTS

Recommendation 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 11 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 on-going basis and via appropriate means (e.g. leaflets, website pages), with clear and straightforward instructions 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.*

RECOMMENDATION 6 – COMMENT:

We seek clarity on the notion that PSPs "confirm [a cardholder's] willingness to conduct internet payment transactions" given that the customer has requested a payment card from their PSP, which automatically provides access to POS terminals, ATMs and ecommerce.

We agree that PSPs should support customers with the use of anti-virus / malware software etc. however we believe that it is unrealistic to assume that a PSP will have the means to continuously update customers, as new fraud trends arise.

Recommendation 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. 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.*

RECOMMENDATION 7 – COMMENT:

7.1 KC We support this recommendation.

7.3 KC We support this recommendation.

7.6 KC We believe that the weakest link, i.e. the least secured stakeholder in the transaction cycle should be liable for fraud losses, where fraud occurs. Where the card issuer invests in costly solutions and provides these solutions to its cardholders, they should not then be held liable if other parties, such as the e-merchant, uses no security measures against online fraud.

We believe that the card schemes, upon which card issuers and acquirers are dependent for the majority of their ecommerce fraud solutions, need to provide more solutions in the market than currently exist. We believe that there needs to be more of an emphasis on the schemes' requirements in this regard.

With regard to the e-merchants specifically, IPSO believes that the recommendation does not necessarily provide for a level playing field, while many merchants operate outside of the EU and as such are not required to comply with these recommendations while the PSPs are under obligation to do so. We believe that there should be greater communication between the EU authorities (especially the ECB) and those involved in setting the standards for similar payments outside of the EU.

7.1 BP IPSO supports the implementation of stronger authentication methods. We believe that an adequate time frame should be allowed, to implement such solutions, as fast-tracking the implementation of same could lead to poor quality security and further fraud losses.

7.2 BP IPSO agrees it makes sense to have one strong authentication method for all activity.

Recommendation 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 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.*

RECOMMENDATION 8 – COMMENT:

In Ireland, consumers are offered a number of options to help verify themselves both at initiation and during their shopping / payment experiences. The banks here continue to support the tools available in the market.

Recommendation 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.*

RECOMMENDATION 9 – COMMENT:

9.1 KC While IPSO agrees with this recommendation in principle, we would note that a restrictive time limit on the customer authentication process could potentially have a negative impact on the consumer experience. Our member banks currently provide realistic time limits to their customers for this purpose, which we believe comply with the recommendation.

The other recommendations are generally part of the current operation.

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.*
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.*

RECOMMENDATION 10 – COMMENT:

We agree with these recommendations and best practices. We would emphasise that it is important for all parties within the transaction cycle chain to monitor and aim to detect fraud, with the onus to do so not entirely the job of the customer's bank.

As before, it is not always possible to detect all fraudulent activity before the fact.

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.*

RECOMMENDATION 11 – COMMENT:

IPSO agrees with this recommendation.

CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION

Recommendation 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 on-going 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.*

RECOMMENDATION 12 COMMENT:

IPSO agrees with these recommendations and best practices.

It should be noted that in addition to the training and awareness campaigns that are carried out by the industry bodies and PSPs, there is also an onus on consumers to understand their responsibilities in keeping their online payments environment safe and in using the security tools made available to them by their PSP.

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.*

RECOMMENDATION 13 – COMMENT:

IPSO agrees with these recommendations and best practices and understands the importance of educating consumers and retailers on current fraud trends and prevention measures.

We believe that the limits set by responsible PSPs in the market should be explained to consumers who should then agree to the limits, or choose to use other payment methods. The use of limits is a valuable tool to mitigating risk, however we believe it should be considered within a basket of potential security tools which can be used to achieve an agreed standard. The industry needs to focus on requirements and outcomes and allow individual PSPs to decide how they meet these goals.

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.*

RECOMMENDATION 14 COMMENT:

IPSO agrees with these recommendations.