PAYMENTS COUNCIL

19 June 2012

DL 020 3217 8437
Martin.Whitworth@ukpayments.org.uk

PAYMENTS COUNCIL RESPONSE TO THE ECB RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS SECURE PAY CONSULTATION

1 ABOUT THE PAYMENTS COUNCIL

www.paymentscouncil.org.uk

The Payments Council is the body with responsibility for ensuring that payment services work for all those that use them in the UK. We work with the financial institutions in the payments industry as well as other stakeholders to drive innovation in payments and implement change so that individuals and businesses have access to payments for their current and future needs.

We have three main objectives:

- To have a strategic vision for payments and lead the future development of co-operative payment services in the UK
- To ensure payment systems are open, accountable and transparent, and
- To ensure the operational efficiency, effectiveness and integrity of payment services in the UK.

We are a membership body with an independent non-voting Chairman. Our Board has four independent directors, who can collectively block any decision that they believe is not in the best interests of those using payment services. Eleven industry directors representing the members also sit on the Board and the Bank of England has a seat as an observer. We are funded by our industry members, which means that we do not place any financial onus on our external stakeholders. We work hard to ensure that the right balance is maintained between all those bodies that we speak to, including the industry members, when reaching any decision that impacts the people who use and rely on payment services.

The Payments Council has three User Forums, made up of a wide range of representative bodies ensuring that the views of consumers, small and medium-sized enterprises (SMEs) and large corporates are delivered effectively. These Forums consider and discuss proposals and offer advice to the Board. Each Forum is chaired by an independent director. In addition, a special liaison group represents the charity and voluntary sector.

The Payments Council has a formal working relationship with a number of the payment schemes in the UK. The schemes are responsible for the day-to-day operating procedures and rules. These are:

- Bacs (incorporating Direct Debit and Bacs Direct Credit schemes);
- CHAPS Clearing Company;
- Faster Payments Scheme Limited;
- Cheque and Credit Clearing Company (including currency clearings);
- The LINK ATM Scheme; and
- Belfast Bankers' Clearing Company.

The Payments Council's Strategic Cash Group provides strategic direction on co-operative (non-commercial) issues for cash; ensuring that the cash people use is distributed efficiently.

2 INTRODUCTION

The Payments Council welcomes the opportunity to respond to this important report.

Set up in 2007, the Payments Council's work to date has focussed on shaping the strategic development of the UK electronic payment schemes, cheques and cash; as well as facilitating and driving innovation activity in the areas of mobile payments, online payments and security. Our emphasis is always on the needs and requirements of those consumers, businesses and other organisations making and receiving payments. We also play an active role in the development of national and international standards for the payments industry.

This experience and expertise makes us well placed to respond to the report. On cards, we have until now played a comparatively less active role and we therefore have a less comprehensive view of our stakeholders' requirements. Therefore, our response on card issues is more limited. Going forward, this is a policy area that the Payments Council will be giving more focus.

Our response falls into two parts. Firstly, we set out a number of thoughts and responses to the general direction and theme of the report. Secondly, we give more detailed responses to specific requirements, key considerations and basic principles of the report.

3 GENERAL THOUGHTS AND RESPONSES

The Payments Council welcomes the aspiration of this report to improve the security of Internet payments. The integrity of online payments is critical to maintaining consumer confidence and the provision of the secure Internet payment services they expect and deserve.

Scope and Addressees

The report does not provide clarity with respect to which parties are within scope and the qualifying reasons for being in or out of scope and should, therefore, be enhanced in this respect. There needs to be a clear statement of scope that clarifies and aligns to terminology within other legislation such as the PSD.

All institutions / entities involved in online payments should be in scope of the recommendations in this report - and this should also include overlay providers who utilise the 'host' account to make payments. The potential threats posed by overlay providers to the integrity of the payments system, e.g. via the need for payees to disclose log on credentials for their internet banking, could compromise the overall security of the payments services. By restricting the scope of the recommendations solely to the PSPs, ignores the part played by other institutions / entities and would seem to place PSPs at a competitive disadvantage.

The recommendations of the report would be much clearer if, where appropriate, there were sections depending on the type of Internet payment service provided by the various institutions (e.g .issuers, acquirers, merchants, etc.)

The list of exclusions from the scope of the report should be revisited, specifically:

- SMS based payments
  These payments are part of the electronic landscape and by excluding them from the recommendations of the report, these un-regulated payment instruments will just become the weakness link.

- Credit transfers via third party overlay providers

These are a growing area within the Internet payments arena and it would therefore be helpful to both existing PSP's and the overlay providers themselves to consider the controls and liability shifts that could be considered for these types of services.

- Corporate cards
  These instruments are a significant element of the online business world, and so should be considered when making recommendation of the secure use of Internet payments services.

Guiding Principles

The report identifies four, sound areas of, guiding principles as the basis for its recommendations.

Risk Assessment

The report identifies the need for PSPs to undertake specific risk assessments for Internet payment. We would contend that financial services institutions current undertake regularly updated risk assessments as a normal part of managing their businesses and the Internet payment services should be viewed as just another area within this risk management activity. Further, by focussing purely on the identification and assessment of risks, this guiding principle omits the important activities associated with the treatment and management of the identified risks. The topic of this guiding principle should be 'Risk Management' rather than 'Risk Assessment'.

Strong Customer Authentication

More clarity is required in the definition of what the report means by 'strong customer authentication'. It needs to establish the principles that should support the claim for an authentication mechanism being declared 'strong', rather than choosing just one possible definition and attempting to provide detailed requirements for that definition.

On a specific point, we would suggest that special care needs to be taken to precisely define the 'mutually independent' concept, when considering two or more elements involved in strong authentication, to ensure that current practices, e.g. involving cards and PINs, are not ruled out.

Transaction Authorisation

We fully support the guiding principle that there is need to have effective processes for authorising transactions and for monitoring transactional activity.

Customer Awareness

We also agree with the requirement that PSPs should engage in customer awareness and education programmes on security issues related to the use of Internet payment services with a view to enabling customers to use such services safely and efficiently. But we would ask that the possibility of using more common, or centralised, customer education mechanisms, in addition to those provide by the individual PSPs, should not be forgotten when considering appropriate channels to customer awareness.

Implementation

We do not believe that the report makes the case to justify its indicated need for regulation to promote the security of Internet payments. Without this compelling case, we foresee that there could be resistance, and delay, to implementation of the various recommendations.

In respect of timescales, there are many recommendations included within the report, some which are more material than others in terms of securing payments through the Internet channel. We would suggest that it may be beneficial to phase the implementation of recommendations, with key timescales aligned to high priority recommendations. Overall, mid 2014 seems ambitious and maybe unrealistic given the scope of those included and scale of improvements required.

Annex 1

With regard to the comments made in Annex 1 about the extension of the PSD to cover payments where only the payer's PSP is located in the EU/EEA (one-leg-out payments), Payments Council believes that such a move would be disproportionate to any benefit to be gained. In particular, articles in the PSD pertaining to the PSD Liability Regime should not be included in any extension (e.g. regarding non-execution, unauthorised execution, liability shift towards the sending PSP) as this would create a disproportionate liability and

risk for payments destined to go outside the Single Market. This would mean that European market players would find themselves at a disadvantage vis-à-vis non-EU/EEA operators, contrary to the objectives set out by the Europe 2020 strategy in terms of competitiveness. A possible extension of the scope of the PSD is one of the elements being considered as part of the Review of the Directive this year. If it emerges during the Review that there is a strong desire to extend the scope of the PSD, the key requirements would be to (1) adopt a uniform approach across all Members States and (2) only take any action in relation to the subset of articles where extension in this way would not be either impossible or have major negative side-effects.

4 PAYMENTS COUNCIL RESPONSE TO THE ECB 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.*

The provision and implementation of a comprehensive security policy is commonly accepted good practice within the payments industry and these policies should encompass clear definitions of roles and responsibilities for all aspects of security, including risk management. It is also evident that such policies should embody all aspects of security, including those associated with Internet payment services.

We see no need for a separate Internet payment services security policy or Internet payment services risk function, as this is included in the normal implementation of an overall security policy, and believe that creating such a separation could in fact cause inconsistencies and weaknesses in the overall security provision. However, such comprehensive security policies should not be solely the domain of PSPs, all participants in the payments chain should follow accepted good practice in security (e.g. as described in the ISO/IEC 27xxx family of standards – particularly ISO/IEC 27001 & ISO/IEC 27002).

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 and the customer.*

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.*

Risk identification and assessment for Internet payment services should be included in the overall environment, and established good practice, of risk management that should be defined within the overall security policy and required of all participants in the payments process, and all information involved in these transactions. Furthermore, these risk

management activities should also be carried out with due consideration for the particular business models and risk appetites of the organisations concerned; i.e. it must be proportionate and appropriate to their customer proposition and risk profiles. Rather than trying to define the requirements of risk identification and assessment in one or two Key Considerations, it would be more useful to reference existing approaches and guidelines in this area (such as the ISO/IEC 27xxx family of standards) that include all aspects of risk management including identification, assessment, treatment, etc.

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.*

We agree that all parties in the payments process should have a comprehensive process in place for the monitoring, handling and follow-up of security incidents, including those associated with Internet payments systems and customer complaints. There is, however, a need to provide more clarity on what is envisioned in terms of notification of incidents and their severities. The priority has to be in containing any incident and protecting customers before notification. In terms of co-operation and engagement with law enforcement, law enforcement needs to have an effective method of dealing with notifications from such organisations. Whilst it would also be useful if there were a common format for reporting

such compromises to an agreed notification point, which is standard across the EU, it should be noted that notification and reporting formats will also be driven by individual organisation's operating model and risk appetite.

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.*

As per previous comments, on Requirement 2, the treatment and management of risks for Internet payment services should be included in the overall environment, and established good practice, of risk management and treatment that should be defined within the overall security policy and required of all participants in the payments process. The security policy will also define the implementation of segregation of duties and environments, and requirements for testing and monitoring.

This requirement, as written, makes the mistake of trying to predetermine what the appropriate mitigation of a particular risk will be by requiring the incorporation of multiple layers of protection. Whilst defence in depth is indeed a viable and useful security principle, it is not the right approach for every situation.

4.2 KC, in particular, falls into the trap of trying to mandate particular implementation solutions, rather than remaining technology agnostic and sticking to a guiding approach; it also risks being counter productive for the more experinced organisations and countries. For example, whilst firewalls, proxies, etc. are potential controls, they do not provide a

viable defence against man in the middle or man in the browser attacks. This document should remain focussed on guiding principles rather than specific solutions.

Testing, rather than auditing, of security, and security controls, should be carried out on a regular basis and by appropriate qualified individuals (e.g. security testers that hold appropriate accreditation), not the risk management function; although risk management may manage such activities. Any identified weaknesses, should be risk assessed, prioritised, and fixed within agreed timescales.

Any outsourced service should be held to an appropriate standard that is aligned to the requirements defined in this report; by the use of appropriate agreements and contracts.

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 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 files 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.*

This requirement needs to be more clearly defined, as it is not clear what may be deemed to be an appropriate level of tracing. For example, it may be determined that an appropriate trace is one that goes back to the end user / customer – this is not achievable as it requires a trace back through any proxies that the customer may be using.

We believe that rather than specifying the actual data fields that are required to be logged, the requirements should rather be to include sufficient information to ensure that the user making any change to the information stored within the system are recorded so that each change can be tracked and both sites (before and after) can be recreated if required. Also, with regard to analysis, the requirement should be that the transaction information can be analysed and that the access to this information, is restricted to individuals that require access to support their business activities.

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 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 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.*

We absolutely acknowledge the importance of proper customer identification, and PSPs in the UK rigorously follow KYC (Know Your Customer requirements). This requirement is unclear, however, in identifying just how a customer should confirm their willingness to undertake Internet payments – and how this information should be retained. Further, we are unable to see what tangible benefits would accrue from the suggestion that customers sign a service contract before transacting online; and also feel that this suggestion may be considered similar to the subject of indemnities, which have been assessed as potentially unfair for consumers by the UK Financial Service Association (FSA) in early 2012 (in the FSA's finalised guidance on Unfair Contract Terms).

More clarity is also required with regard to what constitutes 'necessary identification procedures' and 'adequate identity documents' (6.1 KC), as this KC is too ambiguous as currently worded.

We would also like to seek clarification with regard to the possible conflict between these requirements, as stated, and the EU Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (AML3).

It is our understanding that AML3 allows simplified due diligence (SDD) in certain cases, which include e-money transaction below certain qualifying thresholds. SDD has since proven to be adequate, and therefore there could be confusion for customers and businesses by putting this provision into question. We would also question the inclusion of anti-money laundering in a document that is concerned with security - even though anti-money laundering is a perfectly valid objective.

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.*

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.*

Whilst there can be no question that customer authentication is a key requirement, far more clarity is required here with respect to what constitutes 'strong customer authentication'. Any inconsistencies here between interpretation of the ECB's recommendations and existing legal provisions and industry best practice will only lead to increasing insecurity for consumers and businesses.

In referencing direct debits, more clarity is required on the direct debit being initiated by strong customer authentication. The originator requests the funds and the onus and liability is on them for validation of the identity of the proposer and the account they have provided and signed to debit. The request, therefore, comes from the merchant and strong customer authentication would not reside with the PSP.

Once again, it is not helpful to reference specific technology solutions, such as 3D Secure, as it gives the implication that this is a prescribed solution. It is important to recognise that PSPs will use a range of specific, multiple and simultaneously active layers of defence, corresponding to and commensurate with the level of risk involved in any particular transaction or situation. This specific matching of authentication method to the level of risk

provides an effective way to match the security requirements of both parties in a transaction. Such specific, risk-based, security methods can however only be designed and deployed in a non-prescriptive but flexible, principle-based framework.

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 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.*

The mechanism used for the secure delivery of credentials should be a risk-based decision, which each PSP makes against each customer profile, and specific to the individual market conditions that are being operated in. Prescribing specific delivery mechanisms should not be undertaken without justification, based upon published research. It is also key that the end user is educated in the specific techniques and mechanisms being employed, to be the trusted relationship.

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.*

Once again, whilst supporting the need to establish such rules as described in this requirement, such measures are implementation specific. A series of risk-based decisions by the PSP should establish the appropriate rules for their particular environment.

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) address or IP range during the internet payment session, sometimes identified by geolocation IP checks, 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.*

Security monitoring activities are essential, but decisions regarding the timeliness of this monitoring (real time, near real time, etc.) should be made in a considered and risk-based manner, and should be appropriate to these considerations.

Once again, specific techniques – such as those concerning IP addresses – are being advocated, without justification. The techniques used to perform monitoring should be appropriate, proportionate and decided upon by the PSP.

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.*

The overall requirement for the protection of payment data is sound and one that we would support. However, more clarity should be provided as to what comprises 'payment data', or 'sensitive payment data'; so that everyone may get a greater understanding of what is being required.

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 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 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 *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.*

The possibility of using more common, or centralised, customer education mechanisms, in addition to those provide by the individual PSPs, should not be forgotten. In the UK a number of such initiatives have been established by the Payments Council to do just this; including 'pay_your way' & 'bank safe_online'.

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.*

The management of spending limits is general viewed as a competitive area managed by individual PSPs on a risk-based footing and in appropriate consultation with their customers.

It should be noted that increased reliance on the mobile phone networks (e.g. for SMS alerts) brings with it, its own issues – as demonstrated by the use of phone re-direction and SIM swapping. These, mobile telco, issues will need to be addressed if consumer trust is to be established and maintained.

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.*

The timely provision of transactional information to customers, to allow the to check payments is very important. The mechanisms used to deliver this information should be chosen by the individual PSPs, based on their assessment of the prevailing risks.

5 CONTACT DETAILS

Martin Whitworth
Head of Security

T: +44 (0)20 3217 8437
E: martin.whitworth@ukpayments.org.uk

Payments Council
2 Thomas More Square
London
E1W 1YN

www.paymentscouncil.org.uk