NTT DATA Italia S.p.A.

Sede legale
Viale Cassala 14/A
20143 Milano, Italia
Tel: +39 02 8312 5090
Fax: +39 02 8312 5748
www.nttdata.com/it

European Central Bank
Secretariat Division
Kaiserstrasse 29
D-60311 Frankfurt am Main - Germany

Anticipated by e-mail to ecb.secretariat@ecb.europa.eu

Milan, 19 June 2012

Subject: Public consultation on "Recommendations for the security of internet payments"

NTT DATA EMEA is one of the largest European provider of software solutions for banks and payment institutions.

In particular, our products and services cover a) EU and International Payment processing on standard framework (including SEPA) or innovative channels (as e-Money and MyBank); b) middleware for main network international providers and central systems; c) security layer for card processing and innovative channels (as mobile devices).

NTT DATA EMEA is therefore fully aware of the centrality and criticality of its role in the internet payments industry and welcomes this opportunity for expressing its opinion about the "Recommendations for the security of internet payments" endorsed by the Governing Council of the European Central Bank (ECB) on 11 April 2012.

First of all, we would like to express our general appreciation for the work done in the context of the European Forum on the Security of Retail Payments to facilitate a common knowledge and understanding of issues related to the security of electronic retail payment services and instruments in the Europe.

Generally speaking, NTT DATA EMEA is firmly convinced that a minimum set of harmonized security recommendations will dramatically contribute on fighting payment fraud and enhancing consumer trust in those products and services.

In particular, in developing its own software solutions, NTT DATA has long adopted the substance of recommendations and best practices set out in the document endorsed by the Council.

In this regard, we attach a document setting out our detailed comments on drafted recommendations and best practices. These comments are the result of experience and knowledge gained over many years of dedicated service to the European payments industry.

Moreover, as a key provider of internet payment solutions, NTT DATA is committed to support the Authorities represented in the Forum in contributing to the full implementation of drafted recommendations and best practices by all industry players in the interests of any EU stakeholder.

Sincerely yours,

Andrea Agosti
Head of Security and Risk
Competence Center

Salvatore Borgese
Head of Financial Services
Business Unit

NTT DATA's specific comments on the draft "Recommendations for the security of internet payments"

Comment to specific 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.

Suggestion #1

According to the complexity of PSPs risk management systems and in order to ensure that each PSPs identifies the correct organizational function, it could be useful to underline the required competences for the risk management function in charge of managing security policy on internet payment services. A list of the minimum competences required could be:

- Full understanding of internet payment processes for e-banking, mobile banking, card processing, etc.;

- Full understanding of web based architectures and infrastructures for internet payment services management;

- Full understanding of security solutions for critical data and transactions protection (masking, tokenization, access control, …);

- Full understanding of security governance solutions that can be initiated to define and implement a complete risk assessment process;

- Extensive knowledge of the main operational risk management metrics and reporting requirements for an internal global Risk Management approach.

<u>Suggestion #2</u>

In order to achieve the commitment required on the operational structures and grant compliance with the policy, it could be useful underlining that internet payment services security policy and its reviews should be approved by the authorized administrative body of the PSPs.

<u>Suggestion #3</u>

Main PSPs have already defined and approved security policies, but in many cases these policies are not directly referring to the internet payment services. Defining the main items to be regulated by the specific policy could be useful, as for example:

- *Roles and responsibilities for managing the whole processes related to internet payment services (business / process owner, IT structures involved, back office, risk managers, internal auditors, …);*

- *Risk management processes to be implemented for internet payment services with references to criteria used for threats definition and evaluation, vulnerability assessment, risk evaluation and risk acceptance;*

- *Minimum requirements for security solution aiming to protect critical data and transactions according to mandatory requirements and risk evaluations made by each PSPs;*

- *Security controls implemented for internet payment services with references to control definition, evidences collection and analysis to evaluate security solutions, timing and frequency of implementation;*

- *Standard and best practices adopted within the security of internet payment services.*

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.

Suggestion #1

It could be useful clearly defining that the "senior management" indicated as approver of risk assessments and action plans should include people or Committee with accountability on Risk Management strategy for the PSP.

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 upon 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.

Suggestion #1

It could be useful specifying some requirement for the incident management process:

- *PSPs should define a central incident owner with the responsibility of handling all the phases of the incidents (identification, classification, resolution, follow-up), involving each process owner, according to the incident nature;*

- *The process should be tested at least once a year, it should involve all the third parties implicated in the value chain of the internet payment services and the results of it should be validated by the internal audit department.*

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 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.

Suggestion #1

It could be useful underlining that the principles of "Segregation of Duties" and "Least Privilege" should be implemented by both IT users (System and DB administrator) and end users (applications users) that are exposed, in particular, to the risks of data robbery and alteration.

In order to identify all the systems / applications involved and to grant critical data protection, would be necessary a periodical data classification run by the risk management function in charge.

Suggestion #2

It could be useful to clearly define the role of independent experts that are able to carry out the audits. In particular we suggest to specify that experts can be identified between internal employees and external suppliers. In any case experts have not to be involved into the activities for development, and maintenance of solutions and processes for internet payment services.

<u>Suggestion #3</u>

For the correct attribution of responsibility on the actors involved, it could be useful to underline that the PSP has the direct responsibility to manage only the security measures related to the infrastructure directly managed. PSPs that offer acquiring services can only define contract clauses in order to impose the respect of security requirements.

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, parameterization 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 file scan be evaluated using special tools. The respective applications should only be available to authorized 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.

<u>Suggestion #1</u>

It could be useful to explain the meaning of "parameterization changes". It's necessary to specify if these changes are referred to the parameterization changes (country blocks, payments alerts, ...) made by the user, by the PSP IT administrators or by both. It's necessary to define if the access to transaction data that need to be logged are referred to accesses made by users, by PSP IT administrators or by both. It could be useful to highlight that log file have to be unalterable since their generation, in order to better specify the meaning of "addition, change or deletion".

<u>Suggestion #2</u>

It could be useful to specify that PSPs have to define a minimum conservation period for logs collected. In order to guarantee the availability of data in case of disputes and to avoid an extra cost for PSPs (i.e. implementation of storage infrastructures), 24 months could be considered an adequate period, excepting different risk evaluation performed by the PSP.

<u>Suggestion #3</u>

It could be useful to explain the meaning of "special tools". Maybe it could be useful to define the objectives of special tools:

- Identification of anomalies on anomalous data and according to data correlation schema;

- Implementation of alerts on anomalies identified for internal controls and auditing structures;

- Tracking of all the accesses on log files for forensic analysis.

SPECIFIC CONTROL AND SECURITY MEASURESFOR 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 personalized security credentials;– a step-by-step description of the procedure for the customer to submit and authorize 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 personalized 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 straight forward 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.

In order to avoid misunderstanding, it could be useful to ask each country to define a list of documents that can be considered suitable for customer identification and how to verify the authenticity of the documents.

If the requirements have to be respected also for existing customer, it could be useful to define a maximum period to allow PSPs to adequate their identification, if not already compliant with the new identification requirements.

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 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-DSecure, 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 CVx2should 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 card holder 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.

Suggestion #1

It could be useful to avoid example as 3D Secure into the KC 7.3 because 3D Secure is not considered a strong authentication in its basic configuration.

Suggestion #2

There are exemptions to the adoption of strong authentication by e-merchant, it could be useful to define a limited number of exemptions. Some exemptions could be for small transactions or for specific product categories.

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, personalized 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.

In order to guarantee a common minimum security framework it could be useful to list all the exceptional cases in with strong authentication can by bypassed (e.g. transactions of small amount, specific kind of goods, ...).

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.

Into the KW 9.1, it could be useful to change "few minutes" with "few seconds".

Recommendation 10: Transaction monitoring and authorization

Security monitoring and transaction authorization 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 geo-location 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.

Many Italian PSPs have already adopted transaction monitoring solutions that allow to identity potential fraud events in Near Real Time. Nowadays transaction blocks can be generally implemented only after verification by the contact centers in order to avoid impact on card operability in case of wrong alerts. It could be useful to clarify if transaction monitoring solutions have to allow PSP to block transaction with high fraud risk evaluation in Real Time Mode.

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.

Suggestion #1

It could be useful to highlight that PSPs have to force each e-merchant not to store any payment sensitive data (data for transaction authorization, values and codes for card validation, PIN), according to guidelines defined by international payment circuits.

CUSTOMER AWARENESS, EDUCATION ANDCOMMUNICATION

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 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 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.

Suggestion #1

It could be useful to suggest PSPs offering acquiring services to arrange educational programmes to their e-merchants in order to aware all the parts involved on the criticalities of information security items.

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 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.

<u>Suggestion #1</u>

It could be useful to specify the meaning and the minimum requirements of a " secure environment". It could be also useful to provide a list of information that have to be protected in a "secure environment", that is recalled also in other recommendations.

For example:

- Adoption of the same access control solution both for user and site administrators;

- Protection of sensitive data flow in the end-to-end channel, using secure exchange protocols;

- Protection of sensitive data storage using encryption solutions;

- Periodical Security Assessment, testing external and internal threats that could impact applications and infrastructures involved with internet payments;

- ...

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

<u>Suggestion #1</u>

It could be useful to specify the meaning and the minimum requirements of a "secure environment". It could be also useful to provide a list of information that have to be protected in a "secure environment", that is recalled also in other recommendations.

NTT DaTa
Salvatore Borgese
NTT DATA Italia S.p.A.