Response to the public consultation of the ECB on "Recommendations for the security of Internet Payments"

Provided by ABI

11 June 2012

- **Introduzione**

L'Associazione Bancaria Italiana (ABI) ha predisposto il presente documento di risposta alla consultazione sulle raccomandazioni della Banca Centrale Europea ("*Recommendations for the security of internet payments*", nel seguito "Raccomandazioni") raccogliendo i contributi forniti dagli Associati nonché dal Consorzio ABI Lab (Centro di ricerca e innovazione per la banca), il Consorzio Bancomat (gestore dei circuiti Bancomat e PagoBancomat nonché titolare dei relativi marchi) e il Corporate Banking Interbancario (gestore di un'infrastruttura tecnologica per il corporate banking che consente il colloquio tra i diversi soggetti consorziati in relazione a servizi di pagamento e gestione documentale).

La consultazione in oggetto ha suscitato notevole interesse perché tocca gli aspetti di sicurezza per lo sviluppo dei sistemi di pagamento via internet. Come noto, infatti, tali aspetti sono uno degli elementi chiave per la crescita dei pagamenti elettronici; inoltre, il tema è rilevante anche nell'ottica dell'agenda digitale del settore bancario e del Paese.

L'Associazione accoglie positivamente le 14 Raccomandazioni; si ritiene che la pubblicazione del documento di consultazione rappresenti un'iniziativa di rilievo volta a mantenere elevato livello di attenzione dei PSPs verso i temi di sicurezza dei pagamenti, nell'ottica di contrasto alle frodi e, al contempo, rafforzare la fiducia della clientela verso l'utilizzo del canale internet e delle carte di pagamento. Non sono altresì da sottovalutare le opportunità che si prospettano sia per innovare procedure e soluzioni di identificazione e autenticazione remote offerte dai PSPs, sia per definire un quadro armonico, a livello Europeo, delle misure di sicurezza da adottare a protezione di carte e internet banking.

È in particolare stata apprezzata l'iniziativa di fornire indicazioni armonizzate a livello UE su una tematica che finora è stata lasciata prevalentemente alla sensibilità di singoli Paesi o dei diversi operatori del mercato, sebbene rappresenti un aspetto fondamentale per rendere sostenibile nel medio-lungo periodo i nuovi canali.

- **Osservazioni generali**

Per quanto riguarda l'ambito di applicazione, si condivide appieno l'approccio in merito all'evidenziazione di raccomandazioni per il mondo dei pagamenti online con carta, in linea con quanto accade nel mondo dell'online banking, anche per ragioni di maturità del mercato stesso.

Al riguardo, è importante che il documento tracci con chiarezza indicazioni che si rivolgono non solo ai prestatori di servizi di pagamento ma anche agli esercenti on line e altri operatori non regolamentati.

A questo proposito, rileva notare che se da un lato l'industria bancaria è fortemente attenta agli aspetti di sicurezza dei pagamenti, dall'altro i servizi cosiddetti "third party access to customer accounts" non rientrano

nell'ambito di applicazione delle raccomandazioni e che, se non opportunamente presidiati, possono generare notevoli rischi sotto il profilo della sicurezza delle transazioni e dell'intera operatività online (si veda al riguardo la risposta alla domanda 13 del "Green Paper" della Commissione europea "Towards an integrated European Market for Card, Internet and Mobile Payments" riportata in allegato).

Peraltro, pur considerando le esplicite esclusioni chiarite nella sezione I del documento di consultazione, si renderebbe necessario rafforzare i concetti dei pagamenti multicanale (pc, mobile, tv,...), raccomandando di allineare i livelli di sicurezza per i diversi canali.

Analizzando il documento in considerazione delle caratteristiche dell'attività svolta dai diversi soggetti, si prende atto che l'orientamento prevalente della BCE sembra focalizzato sui servizi di *Internet Banking* e moneta elettronica. Al riguardo si ritiene opportuno chiedere conferma circa il campo di applicazione delle raccomandazioni ai soli servizi di pagamento web based forniti in ambiente competitivo (mono banca).

Altro aspetto dove sarebbe auspicabile un chiarimento è il Contesto di applicazione/esclusione in relazione alla classificazione della clientela imprese e, conseguentemente, contesto di applicazione/esclusione in relazione all'utilizzo di sistema di sicurezza della firma digitale.

Per quanto riguarda i profili di sicurezza affrontati, alcuni specifici elementi proposti, se accolti nella versione definitiva, potrebbero inficiare efficaci investimenti già realizzati dalle banche, in termini organizzativi, tecnologici e dunque rappresentare fonte ingente di costo.

In primo luogo, in relazione al tema della partecipazione degli utenti nel contribuire all'insieme delle misure di sicurezza dei sistemi di pagamenti via internet, nel sottolineare come negli ultimi anni proprio l'utente finale abbia costituito un elemento di debolezza, si apprezza l'enfasi contenuta nel documento, in particolare nelle ultime tre raccomandazioni raggruppate nell'ultima sezione dedicate alla sensibilizzazione della clientela. Si ritiene, tuttavia, che risulterebbe vantaggioso per la sicurezza dell'intero sistema prevedere in forma esplicita, a fronte degli impegni richiesti ai PSPs, modalità di responsabilizzazione della clientela che si riflettano anche nella suddivisione delle relative responsabilità tra PSP e utente. Tale fattore, come anche rilevato dal documento nell'Annex I ("*more clarity is needed regarding the burden of proof … and consumer liability*"), rappresenta infatti uno degli aspetti risultati controversi nell'applicazione della Direttiva sui Servizi di Pagamento (PSD), con il rischio di deresponsabilizzazione di fatto la clientela, ovvero uno degli attori principali dell'intero sistema. Al riguardo, il documento si esprime solo per escludere ogni responsabilità per l'utente nei casi in cui la transazione sia avvenuta senza forme di "*strong authentication*". Si propone di inserire (almeno come suggerimento nei confronti della Commissione Europea) previsioni esplicita di responsabilità da parte degli utenti qualora, pur avendo il PSP dotato il suo sistema di

pagamento di misure rafforzate di autenticazione e di notifica nei confronti dell'utente, quest'ultimo sia venuto meno agli obblighi di comunicazione tempestiva del non riconoscimento di avvenute transazioni.

In secondo luogo si rileva che uno degli aspetti più critici di novità introdotti dal documento in consultazione sia l'estensione della definizione universalmente adottata di "*strong authentication*" includendovi il requisito di non-reusabilità e non replicabilità di almeno uno dei mezzi utilizzati. Pur condividendo il razionale della proposta, si ritiene che tale modifica possa impattare su tecnologie e strumenti oggi già utilizzati da diversi PSPs, rendendo più lunghe, onerose e difficoltose le attività di adeguamento, specie in presenza di un termine previsto oggettivamente breve (circa due anni). Soluzioni che non presentano requisiti di non riusabilità e non replicabilità possono ritenersi comunque adeguati sotto il profilo della sicurezza. Si consiglierebbe pertanto di trasformare tali ulteriori requisiti in "Best Practices" (almeno per un periodo transitorio). A tal fine, si fa anche riferimento al documento dell'*European Payments Councill* (EPC424-10 "*Preventing Card Fraud in a mature EMV Environment*") che individua, come misure di rafforzamento dell'autenticazione dei titolari di carte, anche soluzioni diverse da quelle di "*strong authentication*" e che non prevedono specifici requisiti di non riusabilità e non ripudiabilità.

Da valutare con attenzione anche l'integrazione di tali raccomandazioni con la normativa già esistente in materia e specificamente con il Provvedimento della Banca d'Italia di Attuazione del Titolo II° del D.Lgs. 11/2010 di recepimento della PSD emanato nel luglio 2011.

Inoltre, le attività previste di analisi, *risk assessment*, monitoraggio e controllo, devono potersi integrare con i processi di *risk management*, sicurezza e auditing già in essere nelle singole banche, per evitare duplicazioni di costi e procedure, lasciando alla banca la definizione delle modalità organizzative con cui realizzarle.

Si ritiene importante e pertanto si invita a prestare una particolare attenzione ai pagamenti con le carte dove, in assenza di una chiara disciplina, alcuni soggetti non utilizzano le stesse misure di sicurezza adottate dalle banche, esponendo conseguentemente tutto il sistema a notevoli rischi.

A tal fine, risulterebbe utile inserire (per lo meno in forma di raccomandazione nei confronti della Commissione Europea) chiare indicazioni sulla necessità di comprendere nell'ambito normativo tutti gli attori interessati a qualunque titolo (inclusi i technical service providers e gli e-merchants – questi ultimi spesso interessati dal documento solo da "Best Practices") e prevedere, per favorire la trasparenza verso l'utente e la sua consapevolezza, modalità standard di comunicazione online al cliente delle garanzie di sicurezza dei pagamenti offerti dagli e-merchants.

In aggiunta, si è del parere che potrebbe essere più efficace non fare riferimento a specifiche tecnologie o infrastrutture: lo spirito delle raccomandazioni dovrebbe essere *technologically independent*, al fine di evitare che le raccomandazioni diventino obsolete a seguito della rapida evoluzione di sistemi e *device*. Tra l'altro la differenziazione delle soluzioni tecnologiche porta ad una riduzione del rischio rispetto a potenziali attacchi.

Per quanto riguarda la tempistica, nel documento si cita che i PSPs dovranno essere pronti per il 1° luglio 2014. In merito, si ritiene che la data sia troppo ravvicinata, in considerazione del fatto che si chiede agli intermediari di attuare interventi non sempre immediati e facilmente implementabili.

- **Osservazioni sulle singole Raccomandazioni**

Il documento di consultazione consta di alcune Raccomandazioni che, fermo restando il livello minimo di sicurezza da garantire, - dovrebbe in ogni caso lasciare libertà ai PSPs nello sviluppo tecnologico di varie soluzioni in materia di sicurezza.

Si illustrano di seguito alcune osservazioni puntuali riguardo alle Raccomandazioni:

Raccomandazione 1

A livello generale, si ritiene che le *Key Considerations* (KC) riportate nelle Raccomandazioni 1 (*Governance*) e 2 (*Risk Identification and Assessment*) non siano pienamente in linea con quanto già disposto da Banca d'Italia nel Provvedimento di Attuazione del Titolo II° del D.Lgs. 11/2010 di recepimento della PSD e prevedano al contrario analisi tecnico/applicative/organizzative dai grossi impatti per le banche. Più specificamente, viene qui sancito il ricorso a una funzione indipendente per lo svolgimento di attività di *risk assessment*, superando dunque il carattere di facoltatività presente invece nelle disposizioni nazionali e non evidenziando la possibilità di effettuare certificazioni delle soluzioni adottate a garanzia di una maggiore qualità sotto il profilo della sicurezza.

Key Consideration 1.1

Come già evidenziato nelle osservazioni generali, le misure di sicurezza indicate dovrebbero applicarsi non solo ai PSP ma anche agli altri soggetti che offrono servizi di pagamento, quali e-merchants e operatori non inclusi nelle Raccomandazioni.

Inoltre, risulta complesso e poco chiaro il riferimento al *risk appetite*, in un contesto dinamico e in continua evoluzione, inserito in una logica di obiettivi di comparto.

Key Consideration 1.2

Nell'ambito della definizione di ruoli e responsabilità, andrebbe meglio chiarito il concetto di "funzione di *risk management* indipendente", al fine di evitare impatti organizzativi notevoli rispetto alle funzioni di audit e gestione del rischio già in essere nelle banche; in tal senso, potrebbe essere utile citare, anche a solo titolo esemplificativo, gli standard internazionali di riferimento in ambito sicurezza e IT *Governance* (come la serie ISO/IEC 2700x).

Inoltre, si ritiene importante che le eventuali nuove strutture organizzative e le relative responsabilità identificate dalle raccomandazioni siano adattabili e integrabili anche in funzione della dimensione della banca.

Key consideration 2.1

Si ritiene importante evidenziare che anche i clienti siano responsabilizzati nell'utilizzo dei propri strumenti di pagamento e nelle misure di sicurezza e protezione adottate, prestando le attenzioni e i dovuti accorgimenti ogni qualvolta effettuano una transazione in internet (come poi evidenziato nelle Raccomandazioni successive, dalla 12 alla 14).

Key consideration 2.3

La definizione fornita dal documento di "sensitive data" se non più precisamente dettagliata potrebbe portare a interpretazioni diverse a livello di sistema comportando anche difficoltà nella comunicazione con i clienti e la creazione di aspettative disomogenee. In generale nel documento infatti, alcuni dati possono essere considerati "sensitive" per alcune raccomandazioni e "non sensitive" per altre. Si suggerisce quindi una definizione di "data sensitive" che racchiuda esclusivamente il set minimo di dati realmente critici per la protezione del cliente.

Raccomandazione 3

Si auspica fortemente che l'entrata in vigore di tali Raccomandazioni promuova la costituzione di processi formalizzati e *compliant* tra PSP nei diversi Paesi Europei finalizzati allo scambio di informazioni relative ad attacchi informatici e a incidenti di sicurezza, al fine di massimizzare l'efficacia delle azioni di contrasto e prevenzione delle frodi; tali procedure, infatti, dovrebbero mettere le Forze dell'Ordine nella condizione di avviare tempestivamente investigazioni anche *cross border*. La collaborazione cross border, infatti, è oggi fortemente limitata dalla differenziazione dei contesti normativi a livello locale che non facilitano lo scambio di informazioni a livello europeo In questo contesto, rileva evidenziare la sottoscrizione di una Convenzione ABI – Polizia di Stato, siglata nel Dicembre 2010, finalizzata a contrastare il cybercrime e a promuovere lo scambio di informazioni tra Banche e Forze dell'Ordine in merito a frodi informatiche e incidenti di sicurezza. Inoltre, dovrà essere promossa l'integrazione delle diverse piattaforme presenti nei singoli Stati a supporto della gestione di eventi fraudolenti in ambito monetica, e-commerce ed *e-banking*, per un efficace allineamento tra le Forze dell'Ordine.

Key consideration 3.2

Rispetto alla KC in oggetto, sarebbe auspicabile disporre di una classificazione dei "*major incidents*" menzionati; a tal proposito, si evidenzia per il contesto italiano che, nel caso di incidenti di sicurezza legati all'ambito delle frodi, sono già attive delle procedure di segnalazione da parte delle banche verso Soggetti autorizzati al monitoraggio degli eventi fraudolenti e verso le Forze dell'Ordine mentre, nel caso di incidenti importanti legati al funzionamento dei sistemi informativi, sono già presenti processi di comunicazione con la Banca d'Italia a garanzia della continuità operativa delle infrastrutture.

Key consideration 3.3

Si evidenzia che a livello italiano non esiste a oggi una normativa che regolamenta i processi di *data breach notification* (comunicazioni di violazioni illecite di dati personali sono classificate dall'Autorità Garante per la protezione dei dati personali solo come opportune); pertanto, non si ravvede la necessità dell'introduzione di una norma ad hoc su questo tema, laddove sono già invece attive procedure operative di notifica nei riguardi delle Forze dell'Ordine.

Raccomandazione 4

A livello generale, rileva evidenziare come il settore bancario italiano già da tempo abbia previsto l'introduzione di strumenti e tecnologie in grado di effettuare un presidio continuo degli accessi, della rete e delle operazioni eseguite on line dalla clientela, nell'ottica di rendere sempre più efficace l'attività di rilevazione di tentativi di frode o di transazioni anomale, e di conseguenza, velocizzare le azioni di segnalazione e blocco degli attacchi. In aggiunta, si evidenzia che sono altresì formalizzate nelle banche le procedure per la corretta attribuzione dei profili o delle abilitazioni concesse per l'accesso ai dati e, alla luce delle recenti evoluzioni normative disposte dall'Autorità Garante della Privacy in Italia in materia di trattamento dei dati personali, sono registrati tutti gli accessi degli incaricati ai dati bancari dei clienti correlati a operazioni bancarie. Di conseguenza, si evidenzia che le azioni disposte nelle KC di tale Raccomandazione rappresentano già una buona pratica a livello di sistema.

Key consideration 4.2

Identificazione dei siti ("*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*"): Il requisito è chiaramente comprensibile ed applicabile se riferito a siti web "istituzionali" (portali destinati ai clienti di home-banking o ai titolari di carte di pagamento); non è altrettanto chiara l'applicabilità di tali raccomandazioni nell'interazione con pagine web utilizzate durante transazioni di *e-commerce* da parte di *e-merchants* (ad es. protocolli 3d-secure, che potrebbero, al

contrario, essi stessi risultare non conformi: al riguardo, in fase di autenticazione non risulta essere obbligatoria l'apertura di "*a separate window*" - a differenza di quanto riportato nell'Annex 3 punto 3); spesso, l'interazione avviene all'interno di un frame della pagina del merchant, rendendo di fatto impraticabile la verifica del certificato del sito 3d-secure). Risulterebbe quindi utile un chiarimento in tal senso.

Key consideration 4.4

Per quanto riguarda le azioni di test, pur riconoscendone l'utilità e l'importanza, si ritiene importante evidenziare che le relative modalità organizzative e di implementazione siano definite a livello di singolo PSP. Gli aspetti di rischio coinvolgono le applicazioni nel loro insieme e riferirsi alle sole *risk management functions* per l'esecuzione dei test potrebbe risultare limitativo per l'interpretazione che ne può derivare in ambito PSP, con l'esclusione di funzioni competenti in ambito sicurezza, operative e business, e ai fini della simulazione delle operazioni più rilevanti.

Inoltre la raccomandazione *Tests should also be performed before any changes to the service are put into operation* è nella sua ampiezza generica da un lato poco cautelativa e dall'altro troppo invasiva e va, a nostro avviso, contestualizzata in ragione del numero di cambi cui possono essere sottoposti tali servizi ai Major changes o a quelli che hanno significativi impatti sui livelli di sicurezza.

Key consideration 4.5

Come evidenziato in premessa, si ritiene opportuno specificare il concetto di esperti "indipendenti" deputati alle attività di audit, anche alla luce di quanto contenuto nel recente Provvedimento di Banca d'Italia di Attuazione del Titolo II° del D.Lgs. 11/2010 di recepimento della PSD che non prevede il ricorso obbligatorio a terze parti indipendenti per l'attività di *risk assessment*.

Key consideration 4.6

Si suggerisce di integrare il testo nel seguente modo, ai fini di una maggiore chiarezza: *Contract provisions and clauses with outsourcers should be specified as binding for all components of the chain of sub-contractors and suppliers, as well*.

Key consideration 4.7

Nel mercato italiano la sicurezza dei pagamenti è normalmente "garantita'' dai circuiti e dalle banche (c'è infatti un *redirect* verso i *gateway* di pagamento). Tale impostazione è la stessa del circuito paneuropeo Mybank. Constatiamo però che molti esercenti internazionali che operano sul mercato italiano, malgrado i continui inviti degli issuer, utilizzano procedure che memorizzano i pan della carta, rendendo così debole e vulnerabile la

sicurezza dei dati (in proposito si rimanda alla Key-consideration 11.3, che raccomanda agli esercenti di non conservare i dati).

Inoltre, poiché in caso di problemi le ricadute di immagine andrebbero a danno (indirettamente) anche della banca, si propone di rivedere tale KC considerando la parte del sito web relativa all'effettuazione del pagamento, su cui le banche possono avere presidio diretto, e di monitorare costantemente questa problematica, anche per non inficiare gli investimenti che le banche italiane hanno già fatto in materia di sicurezza.

Si suggerisce di evidenziare per le modalità di attuazione lo standard PCI-DSS del PCI Council.

Key consideration 5.2

Si suggerisce di integrare come segue: *By no means should log files contain sensitive payment data (see Glossary of Terms on page 17)*

Inoltre, dovrebbe essere specificato che tale attività dovrebbe avvenire solo in modalità automatica a garanzia dell'integrità degli archivi.

Best Practice [cards] 5.1

Coerentemente con quanto rilevato per la KC 4.7, l'attuazione di tale previsione non potrebbe essere monitorata dalla banca, in quanto non può avere garanzia delle soluzioni di sicurezza gestite dall'*e-merchants*, e pertanto si suggerisce di stralciarla. Andrebbe piuttosto chiarito il livello di responsabilità distinto fra *merchant* e PSP, senza ribaltare le responsabilità del *merchants* sui PSPs, ma con un dialogo *end-to-end* delle Autorità.

Raccomandazione 6

La presente Raccomandazione non è applicabile a processi di *e-commerce*, laddove la necessità di formalizzare a monte prima del pagamento un contratto che evidenzi le attenzione e le caratteristiche del servizio e che garantisca un preventivo processo di identificazione del cliente, non permetterebbe l'utilizzo esteso dei servizi on line da parte dell'utente Internet. Diversamente, tale KC è in linea con le policy adottate dalle banche per i servizi di *Internet Banking*, che prevedono un'adesione da parte del cliente tramite sottoscrizione di un contratto *ad hoc*.

Key consideration 6.1

Si ritiene importante evidenziare che, tra le modalità di identificazione del cliente da remoto, potrebbero inserirsi anche le opportunità derivanti dalla lettura delle informazioni raccolte nei documenti d'identità elettronica dei cittadini, nell'ottica di una federazione tra pubblico e privato dell'identità e di integrazione dei servizi correlati; a tal proposito, rileva sottolineare la forte attenzione a livello Europeo su questi temi, come testimoniano anche

progetti di ricerca recentemente finanziati e che vedono il coinvolgimento delle banche italiane.

Naturalmente, tali innovazioni tecnologiche e di processo dovrebbero essere accompagnate da adeguate modifiche normative, con particolare riferimento alle disposizioni in materia di anti-riciclaggio. Come infatti rilevato nell'Agenda digitale del sistema bancario italiano persistono vincoli normativi che impediscono direttamente o indirettamente l'esecuzione di processi in modo interamente digitale; ad esempio, la stipula di contratti totalmente da remoto senza riconoscimento fisico del cliente o la gestione della contrattualistica e della documentazione interamente su supporti elettronici. Si auspica dunque a livello europeo un cambiamento normativo che abiliti tali nuove modalità di identificazione dell'utente da remoto.

Key consideration 6.2

Si suggerisce di aggiungere, nella lista delle informazioni da fornire al cliente per l'accesso ai servizi Internet, anche altri elementi relativi al mondo carte (CVx2, PAN, etc).

Inoltre, si propone di evidenziare che i clienti siano informati circa gli aggiornamenti da scaricare e apportare alle proprie soluzioni di protezione (antivirus) nell'ottica di fronteggiare nuovi scenari fraudolenti e nuove tipologie di attacco; a tal proposito, si ritiene importante differenziare la informazioni da fornire al cliente sulla base del servizio erogato (es. attività di e-commerce).

Raccomandazione 7

Come già sottolineato nelle osservazioni generali, uno degli aspetti più critici introdotti nel documento in consultazione è la variazione della definizione universalmente accettata di *strong authentication*; in particolare, si fa riferimento ai concetti di "mutua indipendenza", "non riusabilità" e "non replicabilità" dei mezzi utilizzati che, se introdotti, potrebbero rendere inadeguate diverse modalità di autenticazione forte già in essere nelle banche, con impatti notevoli, sia in termini tecnologici che di costo, ai fini dell'adeguamento. La variazione introdotta, infatti, non prenderebbe in considerazione alcune soluzioni di *strong authentication* efficaci di gestione sicure dell'identità e di contrasto alle frodi già adottate. Si propone dunque di lasciare alla valutazione dei singoli l'adozione di sistemi implementativi con pari o maggiori livelli di protezione, da adottare in via discrezionale (come *best practice*).

Inoltre, tra gli elementi caratterizzanti le soluzioni di *strong authentication*, si suggerisce di aggiungere la firma grafometrica nell'elenco delle tecnologie biometriche, data la notevole diffusione che i dispositivi per la raccolta di tale firma stanno cominciando ad avere nelle banche italiane.

Infine, non è chiaro se il ricorso al doppio fattore sia raccomandato anche al primo livello di autenticazione, ovvero in fase di *log-in* all'*home banking* e

per finalità di carattere solo informativo. Si preferirebbe che tale scelta possa essere effettuata a discrezione della banca per maggiore garanzia di sicurezza o in base alle proprie valutazioni di rischio (possibilità che sembra emergere dalla KC 7.2) e quindi inserita come *best practice*.

Si suggerisce in ultimo di inserire nel "*glossary of terms*" la definizione di "*strong authentication*".

Key consideration 7.3 [cards]

Il ricorso a un'autenticazione forte multi-canale (ad esempio attraverso una tecnologia SMS-based) potrebbe essere suggerita come Best Practice per superare le vulnerabilità delle password statiche presenti nel 3D Secure.

Key consideration 7.7 [cards]

Nell'ambito della gestione della sicurezza sulle carte, si suggerisce di mantenere le presenti raccomandazioni in linea con quanto previsto dallo standard PCI-DSS. Lo scenario ipotizzato prevederebbe infatti la conservazione presso il fornitore del borsellino dei codici CVx2, in contrasto con la PCI-DSS (3.2 - Do not store sensitive authentication data after authorization).

Le osservazioni evidenziate appaiono inoltre rendere più complesso l'uso del borsellino elettronico da parte della clientela. Qualora l'intento della KC sia invece quello di raccomandare al fornitore del borsellino l'utilizzo della strong authentication, si riterrebbe più adatta una formulazione del tipo "*Providers of wallet solutions should support strong user authentication when executing payment transactions via the internet*" e l'indicazione di una liability shift a vantaggio dell'issuer qualora questo non avvenga.

Appare più ragionevole quanto previsto da "SEPA Cards Standardisation (SCS) "Volume" Book of Requirements, Version 6.0" in tema di transazioni ricorrenti (*5.6.2.2.1 Card acceptors, acceptance processing platforms and remote transactions acquirers shall acquire and transmit Card Security Code values or their equivalent. However, for recurring payment transactions where the merchant has stored the card number and the expiry date but not the Card Security Code or its equivalent, the presence of the Card Security Code value, or its equivalent or better means of authentication is only required for the initial transaction.*).

Best Practice 7.1 [cards]

La clausola (*"It is desirable that e-merchants support strong authentication of the cardholder by the issuer in card transactions via the internet"*) sembra essere in contrasto con (notare la differenza tra "it is desirable" e "should require") la KC 7.5 ("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").

Raccomandazione 8

La Raccomandazione riguarda il contesto relativo alla consegna "sicura" degli strumenti di *strong authentication*. Quest'aspetto potrebbe determinare impatti rilevanti e non ci risulta essere univocamente interpretabile quanto raccomandato. Pertanto su questo aspetto si chiede di determinare con maggiore chiarezza:

- se le indicazioni circa le modalità "sicure" per provvedere alla consegna e all'attivazione di uno strumento di *strong authentication* si riferiscono effettivamente alla consegna dello strumento di *strong authentication* (fisico o *software*) che le Banche tipicamente forniscono in aggiunta alle credenziali di accesso (*username-password*) e che talune utilizzano per validare le disposizioni, mentre altre anche per l'accesso;

- nel caso in cui la risposta al punto precedente fosse affermativa, si domanda se tale consegna debba avvenire necessariamente in agenzia/posta o se – laddove si tratti di strumento software – possano essere previste altre forme di invio ed attivazione a distanza; inoltre, nel caso di tali attivazione a distanza, si necessita di sapere se tali processi debbano prevedere l'utilizzo di un elemento consegnato secondo le suddette modalità (agenzia/posta, come ad esempio un codice segreto di attivazione contenuto in una busta a norma) oppure se è sufficiente una *password* prodotta da altro strumento di *strong authentication* consegnato precedentemente al cliente attraverso agenzia/posta, ovvero attraverso un processo che l'issuer ritiene e definisce sicuro.

Key consideration 8.1

In relazione all'indicazione che le password debbano essere fisicamente distribuite, si osserva che ciò avrebbe l'effetto di frenare significativamente l'uso di internet, mentre il ricorso ai canali digitali, debitamente verificati e protetti, diminuirebbe i costi e l'impatto ambientale dell'attività.

L'*activation during shopping* sembra presentare delle difficoltà: le possibilità di completare la transazione originaria sono poche e di conseguenza questa scelta porta all'abbandono dell'acquisto da parte di molti titolari. Da ultimo, non è chiaro quali siano le "eccezioni" di cui si parla nel documento.

Key consideration 8.2

Con riferimento al paragrafo **"***(…) 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"* nella logica di chiarezza delle "definizioni", non si evince chiaramente se la logica è "and" (tutti gli elementi di autenticazione "insieme") o "or" (ne è sufficiente un *subset*).

Key consideration 9.1

Si evidenzia che nell'allegato tecnico al Decreto attuativo del titolo II del decreto legislativo n. 11 del 27 gennaio 2010, di recepimento della PSD - emanato dalla Banca d'Italia nel luglio 2011 - viene indicato come tempo limite di validità per la gestione delle *One-Time-Password* "100 secondi".

Raccomandazione 10

Si chiede di fare maggiore chiarezza in quanto la Raccomandazione in generale chiede ai PSPs di bloccare la transazione in *real-time*, mentre la KC 10.1 parla solo di *detection* e non chiede il blocco della transazione; tra l'altro si fa notare che alcuni PSPs hanno programmi di monitoraggio che agiscono con un'analisi periodica delle transazioni, per cui per quest'ultimi la norma comporta importanti modifiche alle proprie procedure. Di conseguenza, il livello di monitoraggio, periodico o real time, deve essere commisurato al livello di rischio rilevato e al livello di sicurezza richiesto, nonché alle misure di protezione adottate dalle banche e messe a disposizione della clientela.

Si ritiene infine che un importante contributo potrebbe essere dato dagli acquirer, che però non vengono menzionati.

Si chiede inoltre di chiarire se nel caso in cui il PSP utilizzi sistemi di monitoraggio transazioni che non agiscono sulla fase autorizzativa (blocco), se tale attività viene considerata conforme alle raccomandazioni.

Key consideration 11.2

Si ritiene che l'introduzione di livello di sicurezza elevati da adottare nella trasmissione dati end-to-end sia valutata in funzione del livello di rischio associato.

Come già evidenziato nei punti precedenti, per l'ambito carte si potrebbe citare a titolo di esempio lo standard PCI-DSS.

Raccomandazione 11.3 [cards]

Questo punto apparentemente non risulta coerente con la definizione di "*sensitive data*" fornita nel glossario del documento. Alcuni di questi dati (ad esempio indirizzo postale, e-mail, …) infatti risultano necessari al merchant per l'erogazione del servizio e in quanto tali risulta difficile ipotizzare che non vengano archiviati, anche a tutela del merchant stesso.

Raccomandazione 12

Si condivide l'esigenza che vi sia una forte attività di "*education*" alla clientela, in particolare in merito alla gestione sicura delle proprie credenziali digitali, alle modalità più corrette di navigazione e alla protezione delle postazioni di accesso all'Internet Banking, nonché di "*training*" alle

strutture organizzative delle componenti tecniche di ciascun PSP. Tuttavia, si ritiene opportuno rimarcare in primo luogo che tali iniziative non esimono il cliente da un comportamento diligente nell'uso di internet e delle carte di pagamento; in secondo luogo, parte della clientela potrebbe percepire come "invasiva" un'assistenza di tipo tecnologico offerta dalla banca.

Key consideration 12.1

Si ritiene che la clientela debba essere investita di maggiori responsabilità e pertanto si dovrebbe imporre a questi di seguire i dettami suggeriti dall'issuer in materia di sicurezza; inoltre si ritiene che il requisito che l'acquirer chieda ai merchant che lavorano online di adeguarsi ai dettami di sicurezza indicati, dovrebbe essere cogente e non solo "auspicato".

Raccomandazione 14.2

Questo punto apparentemente non risulta coerente con la definizione di "*sensitive data*" fornita nel glossario del documento. Alcuni di questi dati (ad esempio indirizzo postale, e-mail, …) non possono essere mascherati nel momento in cui vengono utilizzati per le comunicazioni.

- **Annex I**

Le raccomandazioni impongono obblighi rilevanti per i PSPs, che meritano approfondimenti dal punto di vista legale, come ad esempio quelli riguardanti la contrattualistica per la fornitura di servizi di internet banking e gli interventi per le comunicazioni relative all'antiriciclaggio.

L'assenza di tali elementi può generare una vera e propria presunzione legale di ordine non autorizzato con conseguente responsabilità in capo ai PSPs e dunque come elemento atto a limitare le responsabilità del cliente. Il documento BCE propone questa precisazione come proposta di modifica alla Direttiva sui Servizi di Pagamento. Al riguardo, mentre si condivide appieno l'indicazione dell'esigenza di una maggiore armonizzazione a livello UE del recepimento delle norme relative alle responsabilità e si condivide lo spunto di rendere maggiormente vincolate le responsabilità sia dei PSPs sia degli utenti merchant all'attuazione delle misure di sicurezza, si chiede di porre estrema attenzione alla proposta di estensione dell'ambito di applicazione della Direttiva.

Infatti ancorché sia evidente che in caso di transazioni online e di e-commerce, le limitazioni geografiche siano prive di senso, ci si deve guardare bene dall'imporre obblighi in capo ai PSPs della UE che essi non sono assolutamente in grado di rispettare poiché il PSP controparte non opera nella UE e dunque è assoggettato a normative diverse. Si rimanda al riguardo alle considerazioni più volte espresse dall'industria bancaria in merito all'estensione delle PSD alle cosiddette "*leg out transactions*" in termini di svantaggio concorrenziale rispetto agli operatori dei paesi non UE.

- **Annex 2**

Come già evidenziato in premessa, si ritiene che quanto elencato e descritto nel presente Annex sia utilizzato solo con finalità esemplificative, al fine di lasciare ai PSP la flessibilità decisionale in merito alle soluzioni tecnologiche di sicurezza da adottare.

Entrando più nel dettaglio dei contenuti, si segnala che in Italia i meccanismi di *strong authentication* si stanno recentemente evolvendo in sistemi di *transaction signing*, ovvero in codici *one-time* generati a partire dai dati della transazione, che aiutano ad evitare gli attacchi di tipo "*man in the middle*". Si suggerisce pertanto di prendere in considerazione anche questi sistemi di sicurezza, più che i "tradizionali" Device Token.

Infine, relativamente al paragrafo "*Software*", si suggerisce di modificare il titolo in "END USER DEVICES". Non è infatti chiara la linea di demarcazione tra le tematiche trattate nel paragrafo precedente ("*Internet Infrastructure and Technology*") e nel paragrafo in oggetto; qualora si decidesse di riportare nel documento elementi di dettaglio su tecnologie/infrastrutture, si suggerisce di focalizzare maggiormente il paragrafo "End user devices" sui problemi e i rischi correlati ai dispositivi dell'utente, arricchendo eventualmente la trattazione con esempi specifici, e di collocare l'analisi sugli aspetti infrastrutturali nel paragrafo precedente.

Allegato: Estratto dalla risposta dell'ABI alla consultazione della Commissione Europea sul "Green Paper – Towards an integrated European Market for Card, Internet and Mobile Payments"

Section 4.1.7 Information on the availability of funds

13) Is there a need to give non-banks access to information on the availability of funds in bank accounts, with the agreement of the customer, and if so what limits would need to be placed on such information? Should action by public authorities be considered, and if so, what aspects should it cover and what form should it take?
Third-parties shall not have access to information pertaining to the availability of funds in accounts without the consent of the account holding bank. Breach of security, data protection and privacy, fraud losses, reputational risks are issues to be considered. Any granting of such access should be entirely secure for both the customer and the PSP holding the account, should be commensurate to the sharing of the costs related to the provision and holding of the account and should be fair as to the responsibilities and opportunities of both PSPs and third parties. In case a strong political willingness to pursue such unsound approach materializes despite the above considerations, a principle of full reciprocity of rights and obligations should be ensured among PSPs and third parties. We point out that in the instructions on "*Implementation of Title II of Legislative Decree 11 of 27 January 2010 concerning payment services*" issued by Bank of Italy in July 2011, it is specified that where an instrument calls for the use of personal security measures (e.g., PINs and passwords), the user is required to take actions aimed at keeping such measures confidential with the aim of preventing unauthorized use of the payment instruments concerned. If the contract between the user and provider of payment services prohibits the former from divulging security codes to third parties, breach of this prohibition constitutes negligent conduct on the part of the user, and thus represents grounds for loss of the exemption from liability set out in the PSD. We consider that this rule is fair and ensures adequate protection of account information, fosters prudent behavior of the customers and awareness of the consequences of misbehavior.