DOCUMENTO DI CONSULTAZIONE DELLA BANCA D'ITALIA SUL RECEPIMENTO DEGLI ORIENTAMENTI DELL'ABE SULLA SICUREZZA DEI PAGAMENTI VIA INTERNET

COMMENTI DI MASTERCARD

MasterCard intende ringraziare la Banca d'Italia per l'opportunità di presentare i propri commenti sul recepimento degli orientamenti dell'ABE sulla sicurezza dei pagamenti via internet del 19 dicembre 2014 ("**Orientamenti**").

MasterCard concorda con l'indirizzo generale delineato dagli Orientamenti e con l'importanza dell'autenticazione forte per contrastare le frodi e per rafforzare la fiducia dei consumatori nei servizi di pagamento via internet. MasterCard, tuttavia, ritiene che l'autenticazione forte per ogni singola transazione non rappresenti una soluzione ottimale né per gli esercenti (i quali sopportano il rischio che i consumatori abbandonino la transazione non completando l'acquisto), né per i consumatori (che preferiscono soluzioni di pagamento facili e al tempo stesso sicure), né per i prestatori di servizi di pagamento ("**PSP**"), né per gli schemi di carte di pagamento. MasterCard raccomanda invece un approccio basato sulla valutazione del rischio (cd. "*Risk Based Assessment/Authentication*", o "**RBA**") grazie al quale, sulla base di vari parametri, si determina se una transazione debba essere sottoposta o meno ad autenticazione forte. In tale ottica l'autenticazione forte rappresenta l'eccezione – e non la regola – al contrario di quanto attualmente previsto dagli Orientamenti.

Per qualsiasi informazione sui commenti riportati, si prega di contattare il Dott. Piero Crivellaro, Vice President Public Policy, Southern Europe, MasterCard Worldwide, Chaussée de Tervuren 198, 1410 Waterloo, Belgio, tel. +32 2 352 4702 e fax +32 2 352 54 44, email piero_crivellaro@mastercard.com

Principi generali sull'autenticazione forte

Prima di fornire commenti specifici sulla consultazione indetta dalla Banca d'Italia e sui vari aspetti di dettaglio degli Orientamenti, riteniamo utile illustrare alcuni dei principi generali di cui raccomandiamo l'applicazione in materia di autenticazione forte e di sicurezza:

1. **Adeguato bilanciamento tra facilità dei pagamenti e riduzione delle frodi.** Sulla base dei *feedback* ricevuti dalle varie parti coinvolte, MasterCard ha sviluppato un approccio secondo cui si deve aver riguardo all'esperienza del consumatore e dell'esercente nello scegliere quando applicare l'autenticazione forte. Grazie al progresso tecnologico, vi sono oggi molteplici dati che consentono di valutare il rischio di ciascuna transazione. Questo è possibile grazie a una serie di parametri quali il riconoscimento biometrico dell'impronta digitale sul dispositivo, l'importo della transazione, la geo-localizzazione, le abitudini di consumo, il profilo della transazione, etc. Prendendo in considerazione tali parametri, è possibile determinare il rischio della transazione e applicare l'autenticazione forte solo nei casi in cui il rischio è elevato (RBA). L'RBA fornisce la protezione che un consumatore e un esercente si aspettano, riducendo drasticamente le frodi senza che sia necessaria l'autenticazione forte per ogni singola transazione.

2. **Necessità di un approccio multi-canale.** Focalizzarsi esclusivamente sui pagamenti tramite *browser* e sul commercio elettronico (*e-commerce*) non corrisponde alle reali necessità di consumatori e esercenti. Vi è una chiara domanda da parte dei consumatori di soluzioni per fare acquisti in

sicurezza e facilità da utilizzare attraverso ogni canale e dispositivo. Un consumatore per esempio può fare acquisti attraverso un'applicazione mobile, chiamare dallo stesso telefono un call-center per pagare una fattura, e utilizzare dalla propria abitazione un *tablet*, un *notebook* o un PC per fare acquisti online. MasterCard, nello sviluppo delle proprie strategie di sicurezza, intende garantire soluzioni che siano da una parte sicure e di facile utilizzo e dall'altra che siano uniformi per tutti questi canali in modo da non ingenerare confusione nel consumatore. Anche in questo caso la nostra strategia ha il duplice obiettivo di: (1) contrastare le frodi e (2) semplificare l'esperienza del consumatore, così da incentivare l'utilizzo degli strumenti di pagamento.

3. **Necessità di neutralità tecnologica.** Si stanno sviluppando rapidamente nuove soluzioni tecnologiche e dispositivi e meccanismi di sicurezza interni a questi ultimi. Notevoli progressi tecnologici sono stati fatti per esempio per stabilire se un dispositivo è effettivamente associato a un determinato consumatore. A fronte di tale complessità, è opportuno determinare degli standard che gli operatori siano tenuti a soddisfare e poi monitorare l'applicazione di tali standard per verificare se tale "asticella tecnologica" possa essere alzata. Non riteniamo opportuno essere prescrittivi in merito a come la tecnologia debba essere utilizzata, mentre è necessario determinare gli obiettivi e gli standard minimi da rispettare. Ciò è ancor più vero dato che cerchiamo di supportare ogni canale e dispositivo, che presentano soluzioni tecnologiche differenti, al fine di mantenere un'esperienza del consumatore e dell'esercente uniforme.

Commenti di MasterCard sul recepimento degli Orientamenti

Inclusione del principio "comply or explain" nel recepimento degli Orientamenti

Come noto, le Raccomandazioni della BCE (*SecuRePay Forum*) per la sicurezza dei pagamenti via Internet ("**Raccomandazioni della BCE**") contengono il principio cd. "*comply or explain*"[1] a beneficio dei PSP e dei circuiti. Gli Orientamenti, tuttavia, non contengono il medesimo principio "*comply or explain*" a beneficio dei PSP (gli Orientamenti prevedono infatti solo che "*le autorità competenti sono tenute a comunicare all'ABE* […] *se sono conformi o se intendono conformarsi agli orientamenti in questione; in alternativa sono tenute a indicare le ragioni della mancata conformità*" – tuttavia tale previsione non è indirizzata ai PSP). Ciò rappresenta una differenza significativa rispetto alle Raccomandazioni della BCE. Riteniamo che i PSP debbano beneficiare del principio "*comply or explain*" sancito negli Orientamenti nella stessa misura in cui i PSP e gli schemi di pagamento ne beneficiano in base alle Raccomandazioni della BCE. Pertanto, MasterCard accoglierebbe favorevolmente l'inclusione del principio "*comply or explain*" nel recepimento degli Orientamenti.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di includere il principio "*complain or explain*" nelle proprie misure di recepimento degli Orientamenti.

Chiarezza in merito alla definizione del termine "supporto"

Non è chiaro cosa si intenda con il termine "supporto" negli Orientamenti 7.3, 7.4, 7.5 e 7.7.

Laddove tale termine dovesse essere interpretato nell'accezione di "supportare, ma non necessariamente applicare" l'autenticazione forte per ogni transazione con carta, MasterCard sarebbe pienamente d'accordo.

Tuttavia, se il termine "supporto" dovesse essere interpretato nel senso di "applicare" l'autenticazione forte a ogni singola transazione con carta, MasterCard nutrirebbe seri dubbi su tale requisito.

[1] Si vedano le Raccomandazioni della BCE, pagina 4, secondo cui: *"Addressees are expected to comply with both the recommendations and the KCs or need to be able to explain and justify any deviation from them upon the request of*

Suggeriamo alla Banca d'Italia di chiarire che il termine "supporto" debba essere interpretato in linea con la risposta alla consultazione indetta dall'ABE sull'Orientamento 7.3. L'ABE ha infatti chiarito che: "[t]*ale Orientamento richiede al PSP emittente di registrare tutte le carte predisposte al pagamento via internet affinché siano tecnicamente pronte ad essere utilizzate con l'autenticazione forte, se richiesto*".[2] Ciò significa che non è necessaria l'autenticazione forte per ciascuna singola transazione.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di chiarire che il termine "supporto" vada inteso nell'accezione di "supportare tecnicamente, ma non necessariamente applicare" oppure "essere tecnicamente predisposto a essere utilizzato, se richiesto" e che l'autenticazione forte non debba essere richiesta per ciascuna singola transazione.

Ratio degli Orientamenti – Necessità di includere il principio di "facilità di utilizzo" per il consumatore (consumer convenience)

Gli Orientamenti menzionano due fondamentali finalità: "*contrastare le frodi nei pagamenti*" e incrementare "*la fiducia dei consumatori nei servizi di pagamento via internet*".[3]

MasterCard apprezza e sostiene tali obiettivi, che sottolineano l'importanza dell'autenticazione forte per contrastare le frodi e aumentare la fiducia dei consumatori nei servizi di pagamento via internet. Tuttavia, MasterCard ritiene che un terzo obiettivo altrettanto importante vada aggiunto: l'autenticazione deve essere di facile utilizzo per i consumatori.

MasterCard è consapevole delle difficoltà pratiche, così come dell'importanza, di un bilanciamento ottimale tra elevata sicurezza e facilità di utilizzo per i consumatori. Riteniamo che gli Orientamenti non raggiungano (ancora) un bilanciamento ottimale tra tali obiettivi. Temiamo che, se recepiti letteralmente, gli Orientamenti finiscano per avere l'effetto non voluto di imporre ai consumatori gravose e inopportune procedure di autenticazione, che potrebbero finire per dissuaderli dall'utilizzo dei pagamenti via internet.

MasterCard ha costantemente promosso da vari anni soluzioni di autenticazione forte basate sul *SecureCode* e altre soluzioni. Il MasterCard SecureCode è un programma concepito per fornire agli esercenti che operano online un livello di sicurezza aggiuntivo consistente nell'autenticazione dei titolari di carta da parte delle banche emittenti e nella protezione da storni (*chargeback*) per transazioni non autorizzate o non riconosciute dal titolare. Il MasterCard SecureCode è conforme ai requisiti di autenticazione forte previsti dagli Orientamenti. MasterCard ha anche adattato il regime di responsabilità per le transazioni fraudolente, esentando da responsabilità gli esercenti che abbiano adottato il SecureCode e garantendo un'esenzione completa da responsabilità (*zero liability*) per i titolari di carta. MasterCard sta sviluppando il SecureCode mediante il lancio di un nuovo programma basato sul "3DSecure versione 2.0", che si avvarrà fra l'altro di password dinamiche e riconoscimento biometrico come fattori di autenticazione.

Oltre al SecureCode, MasterCard ha sviluppato una varietà di altre soluzioni finalizzate a migliorare la sicurezza con l'obiettivo di ottenere un'autenticazione di livello EMV per tutte le transazioni (per esempio, *contactless* NFC, integrate in applicazioni, attraverso *browser* mobili e da PC):

- *Tokenizzazione e MDES (MasterCard Digital Enablement Service)*. I *token* sono numeri di carta che i dispositivi mobili utilizzano al posto del numero di carta impresso sulla carta (PAN). L'MDES è una soluzione che valida la transazione, riconduce il *token* al PAN e inoltra il tutto all'emittente per l'autorizzazione. L'utilizzo dei *token* e dell'MDES consente a MasterCard di offrire un'esperienza di

[2] Si veda la Tavola 3 degli Orientamenti: *Overview of responses to the consultation and the EBA's feedback – Responses to questions in Consultation Paper EBA/CP/2014/31*, pagina 39 degli Orientamenti.
[3] Si veda il Titolo IV – *Objective*, pagina 28 degli Orientamenti.

pagamento più sicura e più facile. Il livello aggiuntivo di sicurezza deriva dal fatto che un token può essere collegato univocamente a uno specifico dispositivo o canale. Se il token viene in qualche modo compromesso e qualcuno tenta di utilizzarlo illegalmente, l'MDES bloccherà la transazione. Se il dispositivo viene smarrito o la carta fisica viene compromessa possiamo rompere il collegamento all'interno dell'MDES tra i *token* e la carta, ed emettere nuovamente il *token* o la carta senza disagio per il consumatore. Simili soluzioni saranno a breve disponibili anche per i pagamenti via *browser*, che si avvarranno dei *secure element* nei *notebook* / PC nei quali i *token* vengono registrati. Il *secure element* fornisce un ambiente protetto per l'esecuzione della transazione, isolando i *token* dal sistema operativo del dispositivo e non registrandoli né su *server* né su *cloud*.

- *DSRP (Digital Secure Remote Payments)*. Il DSRP è un metodo di transazione in cui il consumatore può effettuare acquisti tramite applicazioni (*in-app*) utilizzando un *token*. Il DSRP assicura un livello di protezione analogo a quello delle transazioni EMV anche per i pagamenti tramite applicazioni, proteggendo i consumatori e gli esercenti da transazioni fraudolente e conseguenti storni (*chargeback*).
- *Riconoscimento biometrico*. Il riconoscimento biometrico è molto importante per assicurare un elevato livello di sicurezza fornendo al consumatore un'esperienza di acquisto facile. Per esempio, nel caso di Apple Pay, un PAN tokenizzato unico per ciascun dispositivo e per ciascuna carta aggiunta viene generato e registrato nel *secure element*, ossia in un *chip* protetto dell'iPhone. Quando il pagatore inizia una transazione, deve autenticarsi mediante un codice di sicurezza o attraverso il *Touch ID* con la propria impronta digitale. Tale riconoscimento biometrico, utilizzato congiuntamente alla tokenizzazione, fornisce al consumatore un'esperienza di pagamento facile e sicura. Inoltre MasterCard sta effettuando alcuni test pilota per applicazioni in grado di autenticare i titolari di carta tramite il riconoscimento biometrico del viso e della voce, e sta sperimentando dei braccialetti che autenticano il titolare di carta attraverso il battito cardiaco.

Le soluzioni illustrate dimostrano che un elevato livello di sicurezza dei pagamenti può essere raggiunto senza nuocere all'esperienza del consumatore. Ad avviso di MasterCard, tali soluzioni dovrebbero confluire in standard tecnici riconosciuti a livello internazionale in modo da garantire un uniforme livello di sicurezza e di protezione del consumatore, nonché parità di trattamento tra tutti gli operatori.

La nostra esperienza è tuttavia ben sintetizzata in un articolo di Wikipedia sul "*3-D Secure*", dove si afferma che "[m]*olti utilizzatori vedono il passaggio aggiuntivo di autenticazione come un fastidio o un ostacolo, con un significativo incremento nel tasso di abbandono delle transazioni e una perdita di introiti* [per gli esercenti]".[4] Ciò significa che un aumento dei passaggi di sicurezza che il consumatore deve sostenere per completare una transazione determinerà inevitabilmente tassi di abbandono delle transazioni significativamente più elevati.

MasterCard sostiene e promuove il *SecureCode* e altre misure di autenticazione forte in maniera bilanciata senza perdere di vista l'obiettivo di facilità di utilizzo per il consumatore. Suggeriamo alla Banca d'Italia di adottare un approccio analogo e di rendere la "facilità di utilizzo per il consumatore" una *ratio* esplicita delle proprie misure di recepimento degli Orientamenti.

Si noti che gli Orientamenti prevedono che "[l]*'uso di misure di autenticazione alternative potrebbe essere preso in considerazione per categorie di operazioni a basso rischio pre-identificate, per esempio sulla base di un'analisi del rischio delle operazioni, o che coinvolgono pagamenti di basso valore, di cui alla direttiva sui servizi di pagamento*".[5]

[4] Si veda l'articolo "3D-Secure" (disponibile in lingua inglese) al link http://en.wikipedia.org/wiki/3-D_Secure, dove si afferma che: "*Many users view the additional authentication step as a nuisance or obstacle, which results in a substantial increase in transaction abandonment and lost revenue* [for merchants]".

[5] Si vedano gli Orientamenti 7.5 e 7.7.

Ciò è in qualche misura simile al menzionato approccio RBA che MasterCard sostiene e che è descritto maggiormente in dettaglio di seguito – con la differenza che, ad avviso di MasterCard, i principi dovrebbero essere invertiti: l'RBA dovrebbe costituire la regola, mentre l'autenticazione forte dovrebbe rappresentare l'eccezione (mentre gli Orientamenti prevedono il contrario).

Bilanciamento del principio generale secondo cui l'"inoltro dei pagamenti via internet …dovrebb[e] essere protett[o] da un'autenticazione forte del cliente" in base al rischio, alla responsabilità e alla facilità di utilizzo

Invece di prevedere l'autenticazione forte per ciascuna transazione con carta, MasterCard raccomanda di effettuare una RBA, ossia, come indicato negli Orientamenti, una "*valutazione del rischio relativo a un'operazione specifica tenendo conto di criteri quali, per esempio, i modelli di pagamento del cliente (comportamento), il valore delle relative operazioni, il tipo di prodotto e il profilo del beneficiario*".[6]

Tale approccio è stato adottato in altre giurisdizioni, per esempio, negli Stati Uniti, dove:

- per la clientela non commerciale è sufficiente che le istituzioni finanziarie implementino un approccio multi-livello in linea con il rischio relativo alle transazioni dei consumatori;[7]
- esclusivamente per la cliente commerciale è raccomandata (ma non obbligatoria) l'autenticazione forte (la cd. "autenticazione multi-fattore") per le transazioni via internet.

Secondo MasterCard, un approccio basato sul rischio (RBA) si dovrebbe basare su vari fattori, tra cui:

- *Rischio*. Come indicato dagli Orientamenti, alcuni pagamenti via internet comportano maggiori rischi di altri (in relazione, per esempio, all'ammontare della transazione, alla preventiva autenticazione del consumatore mediante modalità rilevanti per la transazione in questione, alla presenza o meno di indicatori di probabili frodi, etc.). A nostro avviso, l'autenticazione forte dovrebbe essere opzionale e non obbligatoria per i pagamenti che presentino un rischio non elevato.

- *Responsabilità*. Qualora si verificasse una frode a dispetto delle molteplici protezioni adottate dalle varie parti coinvolte, MasterCard disporrebbe di un chiaro quadro di disciplina delle responsabilità per individuare i soggetti responsabili per la transazione fraudolenta; il soggetto responsabile è generalmente l'emittente della carta (in alcuni casi, tuttavia, è l'esercente). Il titolare di carta non è mai responsabile in caso di frode, tranne in alcune circostanze eccezionali.[8] Pur condividendo e promuovendo in termini generali le misure di autenticazione forte, MasterCard raccomanda che un PSP (nello specifico, un emittente di carta) che si assuma la responsabilità in caso di frode possa decidere autonomamente quale livello di autenticazione applicare, purché rispetti alcuni standard minimi e/o non riscontri un livello eccessivo di frodi. Ad avviso di MasterCard, non è necessario

[6] Si veda il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 6° trattino degli Orientamenti.

[7] Si veda il *Federal Financial Institutions Examination Council, Supplement to Authentication in an Internet Banking Environment*, 2011, pagg. 3-4, disponibile al link: http://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf (solo in lingua inglese).

[8] Per quanto riguarda il regime di responsabilità a tutela del consumatore, gli articoli 60 e 61 della PSD prevedono che l'emittente della carta sia in via di principio responsabile per le operazioni di pagamento non autorizzate (il pagatore/titolare di carta è responsabile solamente sino all'importo massimo di € 150, salvo il caso in cui ricorrano circostanze particolari, quali, ad esempio, la mancata notifica dello smarrimento o furto dello strumento di pagamento oppure la mancata conservazione in condizioni di sicurezza delle credenziali di sicurezza personalizzate). L'attuale proposta di PSD2 prevede la riduzione del suddetto importo a € 50; inoltre, la proposta di PSD2, agli articoli 66(1c) nel testo di compromesso del Consiglio del 2 giugno 2015, e 74(2) nel testo di compromesso del Parlamento Europeo del 29 settembre 2015, prevede in modo specifico che il titolare di carta non debba incorrere in alcun rischio di carattere finanziario nel caso in cui l'emittente della carta non richieda l'autenticazione forte del cliente, salvo il caso in cui il titolare di carta abbia agito in modo fraudolento.

obbligare i PSP emittenti a effettuare l'autenticazione forte per ogni transazione laddove si assumano il rischio per frodi (al posto dell'esercente o del titolare di carta). Riteniamo sia più appropriato prevedere requisiti minimi meno stringenti, supportati da un monitoraggio attivo che garantisca il mantenimento del livello di frodi entro limiti accettabili.

- *Facilità di utilizzo per il consumatore.* Come indicato sopra, l'obbligo di autenticazione forte per ogni transazione dovrebbe essere bilanciato in base alla facilità di utilizzo per il consumatore, prendendo anche in considerazione lo scenario della transazione. A titolo esemplificativo, per le transazioni effettuate dai consumatori dal proprio PC di casa potrebbero rivelarsi appropriate quelle soluzioni di autenticazione basate su specifici dispositivi *hardware* (per esempio, lettori CAP o *digipasses*); tali soluzioni, al contrario, non risulterebbero adatte per le transazioni tramite dispositivi mobili "*on the go*" oppure "*in-store*". In termini generali, il rischio di una transazione potrebbe essere determinato sulla base di vari fattori (per esempio, la richiesta di accesso al *wallet* digitale, la verifica che il dispositivo del consumatore utilizzato per effettuare la transazione sia stato previamente associato al medesimo consumatore, la verifica della presenza o mancanza di altri indicatori di rischio, etc). MasterCard propone che i PSP possano prendere in considerazione tali tipologie di fattori e/o l'importo della transazione al fine di applicare la soluzione (in genere meno pratica) dell'autenticazione forte limitatamente alle transazioni con rischio più elevato.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di richiedere l'autenticazione forte solamente per quelle transazioni via internet che l'emittente consideri ad alto rischio sulla base di un'analisi del rischio dell'operazione. MasterCard propone di formulare l'Orientamento 7 come segue: "*L'inoltro dei pagamenti via Internet, così come l'accesso ai dati sensibili relativi ai pagamenti, dovrebbero essere protetti da un'autenticazione forte del cliente* ***sulla base di una analisi del rischio dell'operazione****. I prestatori di servizi di pagamento dovrebbero avvalersi di una solida procedura di autenticazione dei clienti, che sia in linea con la definizione fornita nei presenti orientamenti*".

I pagamenti con un clic (one-click) con i wallet dovrebbero essere consentiti

Quanto esposto sopra sull'opportunità di non richiedere l'autenticazione forte per ogni transazione con carta si applica interamente anche alle transazioni con carta effettuate tramite un *e-wallet*, come per esempio quello di MasterCard (MasterPass). La posizione di MasterCard è contraria all'autenticazione forte sia nel caso in cui il consumatore accede al proprio *wallet* (che sarebbe null'altro che il corrispettivo, nel mondo "fisico", della semplice apertura di un portafoglio contenente delle carte di pagamento, dunque di per sé non certo un'operazione di pagamento) o nel caso in cui effettui l'operazione di pagamento.

Per le soluzioni *wallet*, l'esigenza di garantire la facilità di utilizzo per il consumatore (grazie a un approccio basato sul rischio – RBA – invece di un'autenticazione forte per ciascuna transazione) è fondamentale dato che è proprio in base alla facilità di utilizzo che il consumatore deciderà o meno se utilizzare tali strumenti di pagamento innovativi (ciò a beneficio degli esercenti dal momento che gli *e-wallet* dovrebbero ridurre i casi di abbandono della transazione dovuti a requisiti di autenticazione forte impossibili, o comunque molto difficili, da rispettare ad esempio quando si effettuano pagamenti in mobilità "*on the go*").

Si noti che gli Orientamenti prevedono che "[l']*uso di misure di autenticazione alternative potrebbe essere preso in considerazione per categorie di operazioni a basso rischio pre-identificate, per esempio sulla base di un'analisi del rischio delle operazioni, o che coinvolgono pagamenti di basso valore, di cui alla direttiva sui servizi di pagamento*".[9] Ciò è analogo a quell'approccio RBA che MasterCard ha illustrato *supra* – con la differenza che, ad avviso di MasterCard, i principi dovrebbero essere invertiti: l'RBA dovrebbe costituire la regola, mentre l'autenticazione forte dovrebbe rappresentare l'eccezione (mentre gli Orientamenti prevedono il contrario).

[9] Si veda l'Orientamento 7.7.

Sulla base di ciò, riteniamo che le transazioni con un clic debbano essere consentite per le soluzioni *wallet* quando (i) il titolare di carta è stato autenticato con autenticazione forte al momento della registrazione della carta (oppure al momento della prima transazione effettuata con il *wallet*) e quando (ii) il *wallet* consente – come nel caso di MasterPass – di determinare che il rischio della transazione è basso sulla base di fattori quali il riconoscimento biometrico dell'impronta digitale sul dispositivo, l'importo della transazione, la geo-localizzazione, le abitudini di consumo, il profilo della transazione, etc. Prendendo in considerazione tali tipologie di fattori, è possibile determinare il rischio della transazione e applicare l'autenticazione forte solo laddove il rischio è elevato (RBA).

A tale proposito, è fondamentale che la Banca d'Italia assicuri un trattamento uniforme anche rispetto alle soluzioni *wallet* concorrenti, come PayPal, che beneficerebbero altrimenti dell'esenzione dall'autenticazione forte prevista per i trasferimenti all'interno dello stesso PSP giustificati da un'analisi dei rischi della transazione (Orientamento 7.1).

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di prevedere l'autenticazione forte per le transazioni effettuate con carte già registrate con autenticazione forte in un *wallet* solo laddove il rischio della transazione sia elevato. MasterCard propone la seguente formulazione per l'Orientamento 7.7: "**Gli emittenti** ~~*I fornitori di "wallet solutions"*~~ *dovrebbero* ~~*supportare*~~ ***richiedere*** *un'autenticazione forte del cliente quando i clienti* ~~*procedono all'accesso ai suddetti servizi di pagamento o*~~ *effettuano operazioni con carta via Internet* ***attraverso una soluzione wallet laddove, sulla base di un'analisi del rischio delle operazioni, il rischio è considerato alto***. ~~*L'uso di misure di autenticazione alternative potrebbe essere preso in considerazione per categorie di operazioni a basso rischio pre-identificate, per esempio sulla base di un'analisi del rischio delle operazioni, o che coinvolgono pagamenti di basso valore, di cui alla direttiva sui servizi di pagamento*~~".

Registrazione di una carta in un wallet

MasterCard generalmente raccomanda l'utilizzo di autenticazione forte quando un consumatore registra una carta nel proprio *wallet*, come richiesto dall'Orientamento 7.6.[10] È tuttavia importante notare che vi sono delle eccezioni quando l'autenticazione forte non è ragionevolmente praticabile (per esempio, quando l'emittente non offre una modalità pratica per il fornitore della soluzione *wallet* di richiederla) oppure non necessaria (per esempio, quando i pagamenti successivi con le carte registrate in quei *wallet* sono comunque soggetti ad autenticazione forte al momento della transazione).

La nostra opinione trova conferma nella Guida valutativa della BCE per la sicurezza dei pagamenti via internet di febbraio 2014 (*Assessment Guide for the security of internet payments*, "**Guida Valutativa**"). Infatti, secondo le *Key Considerations* 7.7 e 7.7.1 della Guida Valutativa, il requisito dell'autenticazione forte quando il titolare di carta registra per la prima volta la propria carta è soddisfatto se l'autenticazione forte è richiesta al momento della registrazione, o almeno al momento in cui viene effettuata la prima transazione: "*7.7 KC [cards] For the card payment schemes accepted by the service, providers of wallet solutions should require strong authentication by the issuer when the legitimate holder first registers the card data. 7.7.1 When the legitimate holder first registers card data or at least when the first transaction with the card is initiated, do PSPs provide wallet solutions requiring strong customer authentication by the issuer?*" ("*7.7 KC [carte] Per gli schemi di pagamento con carta accettati dal servizio, i fornitori di soluzioni di tipo "wallet" dovrebbero richiedere l'autenticazione forte dall'emittente quando il legittimo possessore registra per la prima volta i dati della propria carta. 7.7.1 Quando il legittimo possessore registra per la prima volta i dati della propria carta o almeno quando la prima transazione con la carta è inoltrata, i fornitori di soluzioni di tipo "wallet" richiedono l'autenticazione forte da parte dell'emittente?*").

[10] Quale osservazione secondaria, MasterCard rileva che gli Orientamenti prevedono l'applicazione di tale requisito limitatamente ai soli titolari di carta "legittimi"; si tratta presumibilmente di un errore redazionale (in caso contrario, ciò significherebbe che gli emittenti non sono tenuti a eseguire l'autenticazione forte nei confronti di un titolare di carta non legittimato che provi a registrare una carta in un *e-wallet*).

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di non rendere obbligatoria, bensì facoltativa, l'autenticazione forte per la registrazione di una carta in un *wallet*.

La definizione di "soluzioni wallet" dovrebbe essere interpretata estensivamente al fine di garantire la parità di trattamento tra gli operatori

Secondo gli Orientamenti, le "soluzioni "wallet" sono "*soluzioni che permettono al cliente di registrare i dati relativi a uno o più strumenti di pagamento, al fine di effettuare pagamenti con diversi operatori commerciali online*" (si veda il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 8° trattino degli Orientamenti).

MasterCard ritiene che, se interpretata letteralmente, questa definizione non corrisponda adeguatamente al reale funzionamento delle soluzioni *wallet* che sono già offerte sul mercato. Infatti, un'interpretazione letterale di tale definizione non includerebbe i modelli operativi di quei PSP che forniscono soluzioni *wallet* nelle quali la carta non è utilizzata per effettuare pagamenti diretti nei confronti degli esercenti, ma per caricare il conto presso il PSP, con conseguente successivo trasferimento di fondi dal conto all'esercente. Riteniamo che una corretta interpretazione debba qualificare questi PSP come fornitori di *wallet* dal momento che la carta è registrata proprio "*al fine di effettuare pagamenti* (indiretti) *con diversi operatori commerciali online*".

Anche in questo caso è molto importante che la Banca d'Italia garantisca parità di trattamento rispetto alle soluzioni *wallet* concorrenti, come PayPal, che beneficerebbero altrimenti dell'esenzione dall'autenticazione forte prevista per i trasferimenti all'interno dello stesso PSP giustificati da un'analisi dei rischi della transazione (Orientamento 7.1).

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di modificare la definizione di "soluzioni *wallet*" al fine di includere anche quelle soluzioni in cui la carta non viene utilizzata per effettuare un pagamento diretto nei confronti dell'esercente, ma per caricare il conto presso il PSP, con conseguente successivo trasferimento di fondi dal conto all'esercente. MasterCard propone la seguente formulazione per il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 8° trattino degli Orientamenti: "*soluzioni "wallet", soluzioni che permettono al cliente di registrare i dati relativi a uno o più strumenti di pagamento, al fine di effettuare pagamenti con diversi operatori commerciali online~~.~~* ***, incluso il caso in cui gli strumenti di pagamento non siano usati per effettuare un pagamento diretto nei confronti di uno o più operatori commerciali, ma per caricare il conto presso il prestatore di servizi di pagamento, con conseguente successivo trasferimento di fondi dal conto all'esercente***".

Elementi di autenticazione – Riutilizzabilità, replicabilità e idoneità a essere indebitamente sottratti via internet

Le ultime versioni della proposta di PSD2 definiscono l'autenticazione forte quale procedura di autenticazione che soddisfa le seguenti condizioni:

- è "*basata sull'impiego di uno o più elementi classificati nelle categorie della conoscenza, del possesso e dell'inerenza*";
- ciascuno degli elementi utilizzati "*deve essere indipendente, ossia la violazione di un elemento non compromette l'affidabilità degli altri*";
- è "*concepita in modo tale da proteggere la riservatezza dei dati di autenticazione*".[11]

[11] Si veda la proposta di PSD2, articolo 4(1) n. 22 nel testo di compromesso del Consiglio del 2 giugno 2015, e articolo 4(1) n. 30 nel testo di compromesso del Parlamento Europeo del 29 settembre 2015.

Tuttavia, la definizione di "autenticazione forte del cliente" contenuta negli Orientamenti definisce l'autenticazione forte quale procedura di autenticazione che soddisfa tutte le sopra menzionate condizioni e, in aggiunta, la condizione per cui "[a]*lmeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet*" (si veda il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 2° trattino degli Orientamenti).

Pur riconoscendo che le caratteristiche aggiunte alla definizione di autenticazione forte contenuta negli Orientamenti sarebbero in linea teorica auspicabili, MasterCard ritiene che esse creino difficoltà pratiche tali da renderle inadatte a essere incluse nella definizione di autenticazione forte:

- La maggior parte – se non tutti – gli oggetti (fattori di possesso) sono in via di principio riutilizzabili e replicabili.
- Analogamente, non esiste la sicurezza assoluta che essi non possano essere indebitamente sottratti via internet (salva l'ipotesi in cui, ovviamente, internet non sia utilizzato).

Pertanto, le condizioni aggiuntive contenute nella definizione di "autenticazione forte del cliente" contenuta negli Orientamenti, qualora recepite letteralmente, comporterebbero che nessuna procedura di autenticazione per i pagamenti via internet possa essere considerata come autenticazione "forte" ai sensi degli Orientamenti.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di prevedere che la definizione di autenticazione forte richieda che i fattori di autenticazione siano "in via di principio" non riutilizzabili, non replicabili e non idonei a essere indebitamente sottratti via Internet. MasterCard propone la seguente formulazione per il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 2° trattino degli Orientamenti: "***Ove possibile, a****Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet*".

Maggiore chiarezza in merito alla definizione del concetto di "reciproca indipendenza" degli elementi di autenticazione

La definizione di "autenticazione forte del cliente" prevista dagli Orientamenti include i criteri per cui gli elementi di autenticazione impiegati devono essere "*indipendenti, ossia la violazione di un elemento non compromette l'altro o gli altri*" (si veda il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 2° trattino degli Orientamenti).

Pur concordando sulla finalità sottesa a tale affermazione, MasterCard propone alla Banca d'Italia di chiarire che gli elementi di autenticazione debbano considerarsi "indipendenti" quando uno di essi non sia direttamente compromesso per effetto della violazione dell'altro. In altri termini, suggeriamo alla Banca d'Italia di chiarire che il rischio per cui la compromissione di uno degli elementi di autenticazione possa rendere più semplice violare un altro elemento non è condizione sufficiente a ritenere che tali elementi non superino il test di indipendenza. Si consenta di illustrare questo punto utilizzando l'esempio delle soluzioni di autenticazione basate su "*Digipass*":

- Il "*Digipass*" genera una *one-time password* ("**OTP**") dopo che il consumatore ha inserito una password statica (fattore di conoscenza, ossia "qualcosa che l'utente conosce") in uno speciale dispositivo *hardware* associato in via esclusiva allo stesso consumatore (fattore di possesso, ossia "qualcosa che l'utente possiede"). Questi due fattori di autenticazione sono reciprocamente indipendenti.
- Tuttavia, si può ipotizzare che qualcuno riesca illegalmente a compromettere il dispositivo *hardware* "*Digipass*" e a modificarlo (disabilitando le misure anti-manomissione del dispositivo) cosicché, al successivo utilizzo del dispositivo modificato, quest'ultimo trasmetta la password

statica inserita dal consumatore legittimo (ignaro dell'avvenuta compromissione dell'*hardware*) al truffatore.

- Questo esempio dimostra che la compromissione di un dispositivo *hardware* può essere effettuata in modo da agevolare la compromissione degli altri elementi di autenticazione generati dal medesimo dispositivo. Pertanto, è necessario prevedere una definizione più chiara d'indipendenza in quanto anche i fattori di autenticazione ritenuti reciprocamente indipendenti possono, in alcune circostanze, diventare tra loro dipendenti e viceversa.

Esempi analoghi possono essere fatti nel caso di un dispositivo cellulare utilizzato per rilevare e/o verificare caratteristiche biometriche oppure password statiche/PIN. Ciò significa che le soluzioni che prevedono la tracciabilità del dispositivo e l'utilizzo del medesimo per inserire o altrimenti generare altri elementi di autenticazione non superano mai il test di indipendenza? MasterCard ritiene che non sia così, e che tali soluzioni possano considerarsi indipendenti. A nostro avviso, esse sono sufficientemente forti, quantomeno nei casi in cui l'ambiente di esecuzione dell'altro elemento sia ragionevolmente protetto come, per esempio, nel caso del "*secure element*" di uno *smartphone*. MasterCard chiede pertanto alla Banca d'Italia di chiarire che le soluzioni che prevedono tali situazioni siano considerate "indipendenti".

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di chiarire che gli elementi di autenticazione debbano ritenersi "indipendenti" quando uno di essi non sia "direttamente" compromesso per effetto della compromissione dell'altro. MasterCard propone la seguente formulazione per il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 2° trattino degli Orientamenti: "*Inoltre, gli elementi selezionati devono essere reciprocamente indipendenti, ossia la violazione di un elemento non compromette* ***direttamente*** *l'altro o gli altri*".

Si auspica chiarezza in merito alle OTP e agli elementi di autenticazione non forniti dall'emittente della carta

MasterCard auspica dei chiarimenti da parte della Banca d'Italia sulle modalità con cui debbano essere valutate le OTP alla luce della summenzionata definizione di "autenticazione forte del cliente" di cui al Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 2° trattino degli Orientamenti. A nostro avviso, le OTP, di per sé, non autenticano direttamente i consumatori in quanto sono generate automaticamente. Ciò che autentica i consumatori è la procedura di autenticazione che dà loro accesso al dispositivo (o sistema) che genera e/o comunica l'OTP. Si ritiene che si tratti di una precisazione importante in quanto è proprio per questo motivo che alcuni sistemi OTP risultano essere più "forti" rispetto ad altri.

A titolo esemplificativo, si considerino le seguenti tre differenti tipologie di soluzioni OTP, ossia il lettore CAP, un SMS contenente un'OTP oppure un'e-mail contente un'OTP:

- La soluzione del lettore CAP si basa sul possesso di una tessera plastificata/dotata di *chip* (qualcosa che l'utente possiede) e sulla conoscenza di un PIN (qualcosa che l'utente conosce).
- La soluzione tramite SMS si basa sul possesso di una carta SIM associata a un numero di telefono (qualcosa che l'utente possiede) e sul rispettivo PIN del cellulare (qualcosa che l'utente conosce).
- La soluzione tramite e-mail, tuttavia, si basa generalmente solo sulla password statica che viene richiesta per accedere all'account di posta elettronica (qualcosa che l'utente conosce).

Nel primo esempio, entrambi i fattori di autenticazione sono forniti dall'emittente. Nel secondo e terzo esempio, i fattori sono forniti, rispettivamente, dall'operatore di telecomunicazioni e dal *provider* di posta elettronica. Riteniamo che anche i fattori di autenticazione non forniti dall'emittente siano fattori di autenticazione rilevanti in quanto consentono di associare uno specifico dispositivo o account a un determinato utente. Pertanto, tali fattori dovrebbero essere tenuti in considerazione nel valutare il rischio di un'operazione.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di chiarire con quali modalità debba essere valutato il grado di autenticazione dei sistemi OTP e che i fattori di autenticazione non forniti dall'emittente siano ritenuti rilevanti in quanto consentono di associare uno specifico dispositivo o account a un determinato utente. Pertanto, tali fattori dovrebbero essere tenuti in considerazione nel valutare il rischio di un'operazione.

Monitoraggio delle operazioni

MasterCard sostiene pienamente quanto previsto dall'Orientamento 10.1, ossia che i meccanismi per il monitoraggio delle operazioni volti a prevenire, rilevare e bloccare il traffico dei pagamenti fraudolenti debbano essere attivati prima dell'autorizzazione finale del PSP e che le operazioni sospette o ad alto rischio debbano essere oggetto di una specifica analisi e procedura di valutazione.

Tuttavia, MasterCard desidera richiamare l'attenzione della Banca d'Italia sull'articolo 20 (sulla profilazione) del Regolamento generale sulla protezione dei dati ("**RGPD**"), il quale potrebbe limitare la capacità dei PSP di ottemperare a tale Orientamento e di contrastare in modo efficace le frodi.

La definizione di profilazione di cui all'articolo 20 del RGPD è molto ampia e suscettibile di applicazione a numerose attività lecite, quali le attività di monitoraggio e prevenzione delle frodi. In pratica, gli schemi di pagamento e i PSP potrebbero dover ottenere il consenso espresso del titolare di carta per effettuare il monitoraggio delle operazioni e le attività antifrode, salvo il caso in cui tali attività siano espressamente autorizzate dalla legislazione europea o nazionale degli Stati Membri. Ottenere il consenso del titolare di carta non è una soluzione praticabile, considerato che il consenso, affinché sia validamente prestato, deve essere espresso, specifico e revocabile dall'individuo in qualsiasi momento. È pertanto fondamentale che, come minimo, gli schemi di pagamento e i PSP siano espressamente autorizzati nell'ambito della PSD2 a trattare i dati personali ai fini della prevenzione delle frodi.

MasterCard accoglie con assoluto favore gli ultimi testi di compromesso della PSD2 (si veda l'articolo 84) nei quali si opera un ritorno alla previsione sulla protezione dei dati della PSD (si veda l'articolo 79) e si prevede che gli schemi di pagamento e i PSP possano trattare i dati personali per finalità antifrode. Ciò premesso, non è chiaro se tale autorizzazione sia sufficientemente specifica a legittimare i meccanismi di monitoraggio delle operazioni raccomandati dall'ABE e a superare il test previsto dal RGPD.

Al fine di istituire un regime più adeguato e flessibile, MasterCard ritiene che il RGPD e, in particolare, l'articolo 20 debbano rispecchiare un approccio RBA. La profilazione non è di per sé negativa; è l'utilizzo della stessa che può avere conseguenze negative per i consumatori, a seconda del contesto (per esempio, nel caso in cui sia effettuato per finalità di *marketing*). L'implementazione di un approccio RBA garantirebbe una protezione efficace dei dati e al contempo consentirebbe l'utilizzo delle informazioni sull'operazione per scopi di innovazione, incluso l'impiego di sofisticate soluzioni antifrode.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di prendere in considerazione e informare le istituzioni e gli altri stakeholders europei delle potenziali criticità sollevate dalle norme proposte in materia di profilazione, nonché di promuovere l'adozione di un approccio RBA in modo da consentire che il trattamento dei dati personali (relativi alle transazioni) contribuisca a contrastare le frodi nei pagamenti e a rafforzare la fiducia dei consumatori nei pagamenti via internet.

Monitoraggio e segnalazione degli incidenti

MasterCard, nel proprio ruolo di operatore dai forti contenuti tecnologici, è ovviamente fortemente impegnata a innalzare i propri standard di sicurezza e sostiene la necessità di monitorare e segnalare gli incidenti, come previsto dall'Orientamento 3 (inclusi gli Orientamenti da 3.1 a 3.4), al fine di garantire la complessiva fiducia nell'Economia Digitale.

È tuttavia un'esigenza cruciale coordinare e snellire gli obblighi di segnalazione e notifica esistenti in base agli attuali o futuri atti normativi (inclusa la PSD2, la Direttiva NIS e il RGPD). Vi è altrimenti il rischio che gli schemi di pagamento e i PSP siano soggetti a molteplici obblighi di segnalazione degli incidenti a molteplici autorità competenti, che richiedono differenti tipi di informazioni in differenti formati e talvolta persino in lingue differenti. Gli schemi di pagamento e i PSP dovrebbero così dedicare un'enorme quantità di tempo e di risorse a tali segnalazioni, anziché focalizzarsi sull'adeguata gestione e contenimento dell'incidente.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di coordinare il recepimento dell'Orientamento 3 (inclusi gli Orientamenti da 3.1 a 3.4) con l'adozione dell'imminente quadro regolatorio europeo sul monitoraggio e sulla segnalazione degli incidenti (ossia la PSD2, la Direttiva NIS e il RGPD) al fine di assicurare una coerente e uniforme applicazione delle previsioni sulla sicurezza dei pagamenti via internet.

Escludere l'autenticazione forte per le transazioni con carte virtuali

Come illustrato *supra*, l'Orientamento 7 stabilisce il principio generale secondo cui l'autenticazione forte dovrebbe proteggere l'inoltro dei pagamenti via internet. Ciò includerebbe i "pagamenti con carta virtuale" di cui al Titolo I – *Ambito di applicazione e definizioni*, paragrafo 7, 1° trattino degli Orientamenti.[12]

I successivi paragrafi specificano tale principio generale in distinti sotto-Orientamenti in relazione alle diverse tipologie di transazione. Pertanto, per ciascuna di queste, è delineato in modo dettagliato il requisito di autenticazione forte e i suoi limiti di applicazione. Per le carte virtuali, l'autenticazione forte è espressamente prevista solo per il "*processo di generazione di dati della "virtual card""*. L'Orientamento 7.8 prevede infatti che: "[p]*er le "virtual cards", la prima registrazione dovrebbe avvenire in un ambiente sicuro e affidabile. L'autenticazione forte del cliente dovrebbe essere richiesta per il processo di generazione di dati della "virtual card", se questa viene emessa nell'ambiente Internet*".

Ciò significa che (i) la preventiva registrazione su un *browser* o su altri dispositivi, nonché l'accesso alle carte virtuali, deve avvenire in un ambiente sicuro e che (ii) l'autenticazione forte deve essere utilizzata in sede di generazione dei dati della carta virtuale (per esempio, il numero di carta virtuale) su internet. L'autenticazione forte non è invece espressamente richiesta per l'inoltro di ciascuna transazione con carta virtuale.

Le *Key Considerations* 7.9.1 e 7.9.2 della Guida Valutativa confermano tale interpretazione. In relazione alle carte virtuali, la Guida Valutativa prevede la verifica da parte delle Banche Centrali nazionali solamente dell'adozione dell'autenticazione forte per la generazione dei dati delle carte virtuali: "*7.9.1 In the case of the implementation of virtual cards, does the initial registration take place in a safe and trusted environment as per the definition provided? 7.9.2 Is strong customer authentication required when generating virtual card data over the internet?*" ("*7.9.1 Nel caso di implementazione di carte virtuali, la prima registrazione avviene in un ambiente sicuro e affidabile, come richiesto dalla definizione? 7.9.2 È richiesta autenticazione forte per il processo di generazione di dati della virtual card in ambiente Internet?*").

MasterCard concorda sul fatto che il processo di generazione dei dati delle carte virtuali debba essere protetto con autenticazione forte. Tuttavia l'autenticazione forte non dovrebbe essere richiesta per ciascuna transazione, anche in considerazione dei livelli molto contenuti di frodi che caratterizzano le carte virtuali. Occorre considerare inoltre che, nell'ambito delle transazioni commerciali (*business-to-business*),

[12] Il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 7, 1° trattino degli Orientamenti prevede che: "*Gli orientamenti mirano a definire requisiti minimi comuni per i servizi di pagamento via Internet elencati di seguito, indipendentemente dal dispositivo di accesso utilizzato:* […] *[carte] l'esecuzione dei pagamenti con carta via Internet, compresi i pagamenti con carta virtuale, così come la registrazione dei dati relativi alle carte di pagamento per l'utilizzo in "soluzioni di tipo "Wallet""*.

gli utenti di carte virtuali (per esempio, gli impiegati o gli agenti di viaggio che sono autorizzati a utilizzare le carte virtuali per conto di una compagnia) sono spesso tecnicamente impossibilitati a completare le procedure di autenticazione forte.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di chiarire che solo il processo di generazione dei dati delle carte virtuali su internet debba essere protetto con autenticazione forte, e non anche le transazioni con carte virtuali. MasterCard propone la seguente formulazione per il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 7, 1° trattino degli Orientamenti al fine di conformare tale previsione all'Orientamento 7.8: "*[carte] l'esecuzione dei pagamenti con carta via Internet, ~~compresi i pagamenti con carta virtuale,~~ così come la registrazione dei dati relativi alle carte di pagamento per l'utilizzo in "soluzioni di tipo "Wallet*".

Esenzione delle carte aziendali e corporate dall'autenticazione forte

Le carte aziendali e *corporate* dovrebbero essere esentate dall'applicazione dei requisiti di autenticazione forte previsti dall'Orientamento 7 (inclusi gli Orientamenti da 7.1 a 7.9). Tale proposta trova conferma nella Guida Valutativa laddove prevede che agli emittenti sia consentito di non supportare l'autenticazione forte per le carte *corporate* qualora vi sia un'analisi del rischio e un adeguato monitoraggio. Secondo quanto previsto dalla *Key Consideration* 7.3.1 della Guida Valutativa, "[h]*as the card-issuing PSP implemented strong customer authentication for all its cards that are meant to be used on the internet? Are there known exceptions (e.g. corporate cards) and do they benefit from a risk analysis and proper monitoring if there are any issues?*" ("[i]*l PSP emittente di carte ha implementato l'autenticazione forte per tutte le tipologie di carte utilizzabili su Internet? Sono previste delle eccezioni (ad esempio, per le carte corporate) che beneficiano di un'analisi del rischio e di un adeguato monitoraggio nel caso in cui siano riscontrati dei problemi?*").

Pertanto, la *Key Consideration* 7.3.1 prevede espressamente per le carte *corporate* un'esenzione dall'applicazione del principio generale previsto dall'Orientamento 7.3, secondo cui l'emittente deve registrare "[t]*utte le carte predisposte al pagamento via internet affinché siano tecnicamente pronte ad essere utilizzate con l'autenticazione forte, se richiesto*" (si veda il responso alla consultazione indetta dall'ABE, pagina 39 degli Orientamenti). La *ratio* sottesa a tale eccezione risiede nel fatto che le operazioni tra imprese dovrebbero richiedere un livello minore di protezione in quanto presentano un tasso di frodi molto contenuto.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di escludere le carte aziendali e *corporate* dall'ambito di applicazione dell'Orientamento 7 (inclusi gli Orientamenti da 7.1 a 7.9). MasterCard propone la seguente formulazione per l'Orientamento 7: "*L'inoltro dei pagamenti via Internet, così come l'accesso ai dati sensibili relativi ai pagamenti, dovrebbero essere protetti da un'autenticazione forte del cliente. I prestatori di servizi di pagamento dovrebbero avvalersi di una solida procedura di autenticazione dei clienti, che sia in linea con la definizione fornita nei presenti orientamenti.* ***Il presente orientamento e i seguenti orientamenti da 7.1 a 7.9 non si applicano alle carte aziendali e corporate come definite ai sensi dell'articolo 2 del Regolamento (UE) 2015/751***".

Controllo e mitigazione dei rischi

Secondo quanto previsto dall'Orientamento 4, "[i] *prestatori di servizi di pagamento dovrebbero attuare misure di sicurezza in linea con le rispettive politiche di sicurezza, al fine di mitigare i rischi individuati. Tali misure dovrebbero includere più livelli di difesa della sicurezza, di modo che se una linea di difesa viene meno, questa è sostituita dalla linea di difesa successiva ("difesa in profondità")*".

MasterCard approva e sostiene il suddetto Orientamento, il quale sottolinea l'importanza di utilizzare molteplici livelli di sicurezza. A tal riguardo, MasterCard sta implementando SafetyNet, uno strumento globale concepito per ridurre i rischi di hackeraggio (*cyber hacking*) nei confronti di banche e di soggetti che

processano le operazioni (*processors*). SafetyNet è progettato in modo da prevenire i potenziali attacchi prima che abbiano luogo e, in alcuni casi, prima ancora che il PSP o il *processor* ne venga a conoscenza, sfruttando un sistema di difesa a più livelli. SafetyNet è complementare rispetto agli strumenti del PSP emittente, ma aggiunge un nuovo livello di protezione al sistema di pagamento. SafetyNet monitora differenti canali e aree geografiche, e fornisce il livello di supporto più adeguato attraverso l'utilizzo di algoritmi sofisticati.

L'utilizzo di finestre integrate (inline windows) per l'autenticazione 3D Secure dovrebbe essere consentito

L'Orientamento 12.5 prevede che "[i] *prestatori di servizi di acquiring dovrebbero richiedere agli operatori commerciali online di separare chiaramente i processi relativi ai pagamenti da quelli inerenti il negozio online onde rendere più agevole per i clienti identificare quando comunicano con il prestatore di servizi di pagamento e non con il beneficiario (per esempio reindirizzando il cliente e aprendo una finestra separata in modo che il processo di pagamento non venga visualizzato all'interno di un contesto di commercio online)*".

MasterCard desidera richiamare l'attenzione della Banca d'Italia sul fatto che tale Orientamento non è in linea con l'obiettivo dichiarato di accrescere la fiducia dei consumatori nei pagamenti via internet. Infatti, è proprio l'utilizzo di sezioni (*frames*) all'interno del website dell'esercente a dare al titolare di carta quel senso di sicurezza di trovarsi ancora sul sito web dell'esercente e di non essere stato oggetto di *phishing*. Inoltre, richiedere agli esercenti di separare nettamente i processi relativi ai pagamenti da quelli relativi alla fruizione delle funzioni del website potrebbe seriamente compromettere l'esperienza dell'utente e la facilità di utilizzo. Inoltre, i sistemi di blocco dei *pop-up* generalmente bloccano qualsiasi nuova finestra, comportando un tasso di abbandono dell'operazione estremamente elevato.

Riteniamo pertanto che la *ratio* dell'Orientamento 12.5 debba indirizzare la Banca d'Italia a prevedere che i processi relativi ai pagamenti siano visualizzati in modo chiaro e trasparente per il cliente così da rendere più facile a quest'ultimo comprendere quando comunica con il PSP e non con l'esercente, senza dover necessariamente essere re-indirizzato verso finestre o siti web separati.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di recepire l'Orientamento 12.5 in modo da assicurare che i processi relativi ai pagamenti siano visualizzati in modo chiaro e trasparente al fine di rendere più facile per i clienti comprendere quando comunicano con il PSP e non con l'esercente. MasterCard propone la seguente formulazione per l'Orientamento 12.5: "*I prestatori di servizi di acquiring dovrebbero richiedere agli operatori commerciali online di ~~separare in modo~~* ***fornire una visualizzazione*** *chiar~~o~~**a de**i processi relativi ai pagamenti ~~da quelli inerenti il negozio online onde~~* ***e*** *di rendere ~~più~~ agevole per i clienti identificare quando comunicano con il prestatore di servizi di pagamento e non con il beneficiario ~~(per esempio reindirizzando il cliente e aprendo una finestra separata in modo che il processo di pagamento non venga visualizzato all'interno di un contesto di commercio online)~~*".

Le migliori prassi non dovrebbero essere rese obbligatorie

La Banca d'Italia non dovrebbe rendere obbligatorie le migliori prassi ("**MP**") allegate agli Orientamenti perché ciò comporterebbe un'indebita restrizione per i PSP, oltre a non essere richiesto dagli Orientamenti stessi. L'ABE ha espressamente affermato che le MP sono solamente consigliate e non ne è richiesta l'implementazione.[13]

[13] Si veda il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 8 degli Orientamenti: "[i] *presenti orientamenti, oltre ai requisiti riportati di seguito, forniscono altresì esempi delle prassi migliori (allegato 1) che i prestatori di servizi di pagamento sono invitati, ma non sono tenuti, a seguire*"; si veda l'Allegato 1, pagina 22 degli Orientamenti, ove si prevede che "[o]*ltre ai requisiti di cui sopra, i presenti orientamenti descrivono alcune procedure che i prestatori di servizi di pagamento e gli operatori di mercato coinvolti sono invitati, ma non tenuti, ad adottare. Per facilità di riferimento, i capitoli cui si applicano le migliori prassi (MP) sono indicati in modo esplicito*"; si veda la Tavola 3: *Overview of responses to the consultation and the EBA's feedback – Responses to questions in Consultation Paper*

Rendere le MP obbligatorie significherebbe prevedere regole sulla sicurezza dei pagamenti via internet più restrittive di quelle degli altri Stati Membri. Ciò ostacolerebbe lo sviluppo dell'industria italiana dei pagamenti, con ciò determinando:

- L'adozione di procedure di autenticazione più gravose che aumentano la difficoltà nei pagamenti (*friction*) e l'abbandono dell'acquisto.
- Uno svantaggio competitivo per i PSP italiani che sarebbero soggetti a regole più restrittive rispetto a quelle applicabili ai PSP stabiliti in altri Stati Membri.

A titolo esemplificativo, si considerino le seguenti MP:

- **Migliore Prassi n. 4**: Secondo la MP4, il cliente "*potrebbe sottoscrivere un contratto di servizio dedicato per lo svolgimento di operazioni di pagamento via Internet, anziché le condizioni contrattuali incluse in un contratto di servizio generale più ampio con il prestatore di servizi di pagamento*". Riteniamo che la MP4 imponga un obbligo aggiuntivo gravoso e inopportuno per i clienti e i PSP, senza apportare un reale beneficio per i clienti. Qualora la *ratio* sottesa alla MP4 fosse quella di rendere noti al cliente i termini e le condizioni applicabili alle operazioni di pagamento via internet, tale risultato potrebbe essere conseguito indicando separatamente i termini e le condizioni nel contratto di servizio generale, senza duplicare i contratti. Ciò sarebbe infatti costoso per gli emittenti, in particolare a seguito dell'entrata in vigore dei livelli massimi di commissioni interbancarie previsti dal Regolamento (UE) 2015/751 (Regolamento sulle commissioni interbancarie multilaterali) che ha drasticamente ridotto per gli emittenti gli introiti derivanti dalle commissioni interbancarie multilaterali.

- **Migliore Prassi n. 8:** La MP8 richiede che l'autenticazione forte "*includ*[a] *elementi in grado di collegare l'autenticazione di un importo specifico e del beneficiario*". La MP8 riproduce sostanzialmente la previsione della PSD2 che richiede di includere nell'autenticazione forte elementi che colleghino l'autenticazione a un importo e a un esercente specifico nella forma di un codice dinamico.[14] La Banca d'Italia non dovrebbe, allo stato attuale, imporre un simile obbligo ai PSP, i quali dovrebbero altrimenti effettuare investimenti significativi per adeguare i propri sistemi (diversamente dai PSP di altri Stati Membri). Qualora divenisse obbligatorio prevedere elementi che colleghino in maniera dinamica l'operazione a un importo o a un esercente specifico, sarebbe opportuno ricevere ulteriori chiarimenti sulla definizione di tali elementi. Per esempio, questi elementi dinamici dovrebbero essere generati dallo stesso dispositivo *hardware* in cui il titolare della carta inserisce manualmente le proprie credenziali o sarebbe sufficiente introdurre un sistema a valle che li generi? Nel caso di un'operazione tramite carta, il codice di approvazione dell'autorizzazione da parte dell'emittente potrebbe essere considerato un elemento dinamico – come MasterCard ritiene che debba essere?

La proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di non rendere obbligatorie le Migliori Prassi allegate agli Orientamenti. Qualora la Banca d'Italia dovesse rendere obbligatoria la MP8, dovrebbe almeno prevedere che, in caso di operazione tramite carta, il codice di approvazione dell'autorizzazione da parte dell'emittente possa essere considerato un "elemento dinamico".

Dovrebbero essere pubblicati studi ed esempi di esenzione dall'obbligo di autenticazione forte

---

EBA/CP/2014/31, pagina 36 della versione inglese degli Orientamenti, che recita ""[a]*s explained in the annex of the guidelines, best practices are only encouraged and not required to be implemented*" ("[c]*ome spiegato negli allegati agli orientamenti, le migliori prassi sono solamente suggerite e non ne è richiesta l'implementazione*").

[14] Si veda la proposta di PSD2, art. 87(1a) del testo di compromesso del Consiglio del 2 giugno 2015 e art. 87(2) del testo di compromesso del Parlamento europeo del 29 settembre 2015.

Secondo gli Orientamenti, l'"*analisi del rischio dell'operazione* [è] *la valutazione del rischio relativo a un'operazione specifica tenendo conto di criteri quali, per esempio, i modelli di pagamento del cliente (comportamento), il valore delle relative operazioni, il tipo di prodotto e il profilo del beneficiario*" (si veda il Titolo I – *Ambito di applicazione e definizioni*, paragrafo 12, 6° trattino degli Orientamenti).

Ciò è in qualche modo simile all'approccio RBA che MasterCard ha descritto *supra*. Per assicurare uniformità nell'applicazione degli Orientamenti e nel livello di protezione del consumatore tra i vari Stati Membri, desidereremmo conoscere nello specifico quali tipologie di operazioni a basso rischio possano essere esentate dall'applicazione dei requisiti di autenticazione forte sulla base di un'analisi del rischio dell'operazione.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di pubblicare gli studi oggetto di discussione a livello europeo con le altre Banche Centrali nazionali oppure altri esempi in modo da fornire indicazioni sulle esenzioni dall'obbligo di autenticazione forte.

I termini per il recepimento degli Orientamenti dovrebbero essere posticipati in misura adeguata

Al fine di ottemperare ai principi degli Orientamenti, i PSP dovrebbero avere a disposizione più tempo per adeguare i propri sistemi ed effettuare gli investimenti finanziari necessari.

Attualmente le banche sono soggette alle Raccomandazioni della BCE, già trasposte nel quadro normativo nazionale applicabile alle banche (Circolare della Banca d'Italia n. 285/2013). Pertanto, le banche possono attualmente decidere di conformarsi alle Raccomandazioni della BCE oppure di motivare un'eventuale inottemperanza. Al fine di assicurare un uniforme livello di protezione dei consumatori e parità di condizioni concorrenziali tra tutti i PSP operanti in Italia, riteniamo che le misure di recepimento degli Orientamenti in Italia debbano applicarsi a tutti i PSP nel rispetto della stessa tempistica.

Proposta di MasterCard: MasterCard suggerisce alla Banca d'Italia di concedere a tutti i PSP il termine di un anno per adeguare i propri sistemi ed effettuare gli investimenti finanziari necessari.