DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

# L'ABF sull'autenticazione "forte" delle operazioni di pagamento tramite mobile wallet

24 Novembre 2021

**Roberto Ferretti**, Partner, Annunziata & Conso

DB non solo diritto bancario

**Roberto Ferretti**, Partner, Annunziata & Conso

**Roberto Ferretti**

Roberto Ferretti è partner del network Annunziata&Conso, dove svolge attività di consulenza nei settori del diritto bancario, dei servizi di pagamento e di investimento, antiriciclaggio e commerciale. È membro dell'Organo decidente di Milano dell'Arbitro Bancario Finanziario (ABF) e mediatore dell'Organismo di Conciliazione Bancaria. È Presidente e membro e del Comitato scientifico dell'Association Européenne pour le Droit Bancaire e Financier (AEDBF) e membro dello European Law Institute.



**1. La questione sottoposta al Collegio di Coordinamento e il principio di diritto da questo affermato**

Il Collegio di Coordinamento è stato recentemente chiamato a chiarire le modalità di applicazione dei requisiti di autenticazione "forte" delle operazioni di pagamento disposte tramite una carta di pagamento "tokenizzata" in un *wallet* attivato su un dispositivo mobile.

La questione è stata sottoposta al Collegio di Coordinamento da quello di Bari, al quale era stato presentato il ricorso di un cliente che chiedeva la restituzione di due operazioni di pagamento disposte tramite *mobile wallet* e da lui disconosciute. Più precisamente, il Collegio rimettente ha rilevato la complessità del tema della prova dell'autenticazione delle operazioni di pagamento effettuate tramite *mobile wallet* e il diverso orientamento seguito al riguardo dai Collegi territoriali.

Con la decisione n. 21285 dell'11 ottobre scorso, Il Collegio di Coordinamento dell'ABF ha deciso la controversia in favore del ricorrente, affermando al contempo il seguente principio di diritto: "*L'utilizzo di un* wallet *affidato a un terzo gestore per l'esecuzione di operazioni di pagamento [mediante una carta] non esime l'intermediario, in qualità di prestatore di servizi di pagamento, dall'onere di fornire prova dell'autenticazione forte delle operazioni compiute. La prova non può limitarsi alla fase di c.d. tokenizzazione della carta nel* wallet, *ma deve riguardare anche la fase esecutiva delle singole operazioni, non potendosi ritenere implicito che le transazioni siano state correttamente autenticate dal fatto che le stesse risultino autorizzate o comunque dalla sola evidenza che siano state effettuate in modalità* contactless".

**2. La tokenizzazione delle carte di pagamento**

La motivazione della decisione del Collegio di Coordinamento contiene – oltre ad una precisa ricostruzione del dato normativo applicabile - un'accurata descrizione del processo di *tokenizzazione* della carta di pagamento. Tale processo consiste in una procedura informatica grazie alla quale i dati di una carta di pagamento fisica sono registrati in un'applicazione per dispositivo mobile (c.d. *wallet*). Il numero della carta di pagamento (PAN) viene sostituito con un codice numerico (detto *token*) che può essere utilizzato solo in quel *wallet* e solo da quell'utente. Conseguentemente, quand'anche un malintenzionato entrasse in possesso del *token*, non potrebbe utilizzarlo per fare pagamenti fraudolenti in altri contesti (ad es. in un altro *wallet* o su un sito di commercio elettronico).

La più diffusa tipologia di *mobile w*allet (nota come *pass-through wallet*) si basa su un contratto fra il gestore del *wallet*, che solitamente non è un prestatore di servizi di pagamento ma una Big Tech, e l'intermediario che ha emesso la carta.

I *wallet provider* offrono solitamente due modalità di tokenizzazione delle carte. Nel primo caso l'utente opera all'interno del wallet e vi inserisce i dati della carta fotografandola con la fotocamera del dispositivo mobile o inserendo manualmente i suoi dati. Nel secondo caso, l'utente si serve dell'applicazione di *mobile banking* dell'emittente installata sul dispositivo mobile, che contiene già i dati carta, e si limita ad "aggiungere" la carta al *wallet* tramite tale applicazione. Una volta completato il processo di autenticazione, il telefono cellulare consente di utilizzare la carta tokenizzata come se fosse una carta *contactless*.

**3. *Mobile wallet* e autenticazione forte dell'utente**

Come affermato dal Collegio di Coordinamento, a prescindere dalla modalità con la quale la carta di pagamento viene digitalizzata, sia la digitalizzazione stessa, sia il suo successivo utilizzo devono rispettare i requisiti di autenticazione forte previsti dall'art. 97 della PSD2, dall'art. 10-*bis* del d.lgs. n. 11/2010 e dagli RTS dell'EBA ([1]). Tali fasi devono, pertanto, essere considerate separatamente al fine di verificare il rispetto di tali requisiti.

Quanto alla prima, è opportuno premettere che anche l'EBA – così come la decisone in commento – ha chiarito che essa è un'operazione condotta da remoto che può comportare il rischio di frodi e di altri abusi e, per questo motivo, deve rispettare i sopra richiamati requisiti di autenticazione forte (cfr. la QA 2019_4910), a meno che non trovi applicazione una delle ipotesi di esenzione prevista dagli RTS. Come ben chiarito dal Collegio di Coordinamento, inoltre, questa autenticazione è gestita dall'intermediario che ha emesso la carta di pagamento, che ne può scegliere tipologia e caratteristiche tra quelle supportate dal *wallet provider* e dal circuito cui la carta stessa appartiene. In questa fase del processo, infine, il secondo fattore necessario al fine di ottenere l'autenticazione forte dell'utente consiste nell'invio all'utente via SMS di una password "usa e getta" (detta OTP) o in meccanismi analoghi (ad es., una notifica *push* recapitata all'utente tramite l'applicazione di *mobile banking* dell'intermediario o un codice di attivazione "usa e getta" generato dalla medesima applicazione o da un altro dispositivo).

Nella seconda fase, quella, cioè, in cui viene avviato il pagamento, l'autenticazione avviene interamente sul *device* dell'utente e i due fattori necessari ai fini dell'autenticazione forte dell'utente consistono (i) nel possesso del *device* sul quale è stato attivato il *mobile wallet* contenente la carta tokenizzata e (ii), alternativamente, in un elemento di inerenza (quale il riconoscimento facciale o dell'impronta digitale) o in un elemento di conoscenza (quale un codice statico in precedenza scelto dall'utente). Al momento del pagamento la combinazione di questi due fattori genera il codice univoco dinamico di autenticazione, che deve rispettare i requisiti previsti dall'art. 4 degli RTS e viene inviato al POS del beneficiario. Ne consegue che gli ordini di pagamento generati utilizzando una carta tokenizzata sono trasmessi dal *mobile wallet* al POS del beneficiario "già autenticati" e, per questo motivo, il POS non chiede la digitazione del PIN associato alla carta di pagamento.

Alla luce di quanto precede, si comprende che, nel caso di operazioni di pagamento disposte mediante carte di pagamento tokenizzate, il processo di autenticazione forte dell'utente viene integralmente gestito tramite i servizi tecnici offerti dal *wallet provider* all'emittente sulla base dell'accordo di cui si è detto sopra e le credenziali dell'utente sono pertanto gestite dal *wallet provider* medesimo.

Tale esternalizzazione del processo di autenticazione è stata ritenuta conforme con l'art. 97 della PSD2 e con gli RTS dall'EBA, la quale ha avuto modo ci intervenire più volte sull'argomento rispondendo ai quesiti postile ([2]).

D'altro canto, non si può non considerare che – come ben evidenziato dalla decisione del Collegio di Coordinamento che si commenta – tale esternalizzazione pone all'emittente delicati problemi di prova

1 Regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. V., in particolare, gli artt. 10-18.

2 Cfr., in termini generali, la *Opinion of the European Banking Authority on the elements of strong customer authentication* under PSD2 del 21 giugno 2019 (https://www.eba.europa.eu/file/104475/) e, tra le altre, le seguenti risposte a quesiti rinvenibili anch'esse sul sito dell'EBA (https://www.eba.europa.eu/single-rule-book-qa): 2019_4560, 2019_4651, 2019_4875, 2019_4910, 2019_4937 e 2019_4984.\

dell'autenticazione qualora l'utente disconosca un'operazione di pagamento eseguita mediante mobile wallet e ne chieda il rimborso.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

# Scopri il nuovo dirittobancario.it