Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Decisione N. 21285 del 11 ottobre 2021

COLLEGIO DI COORDINAMENTO

composto dai signori:

(CO) LAPERTOSA	Presidente
(CO) LUCCHINI GUASTALLA	Membro designato dalla Banca d'Italia
(CO) DE CAROLIS	Membro designato dalla Banca d'Italia
(CO) GRANATA	Membro di designazione rappresentativa degli intermediari
(CO) VASCELLARO	Membro di designazione rappresentativa dei clienti

Relatore: GRANATA ENRICO

Seduta del 04/10/2021

FATTO

Il ricorrente, titolare di una carta di credito e di una carta bancomat, espone di aver subito in data 11.08.2020 due truffe telematiche di € 390,00 ciascuna.

Riferisce nello specifico:

- che in data 11.08.2020 gli veniva richiesto via *mail* un aggiornamento dei dati della carta di credito e del relativo conto corrente "*consistente in un mero click*";
- che alle ore 16:00 del giorno successivo veniva avvisato dall'Ufficio frode dell'intermediario convenuto che l'11.08.2020 era stato disposto, tramite la carta bancomat, un pagamento *on line* a sua insaputa, rivelatosi poi essere un'operazione di € 390,00, subito disconosciuta;
- che l'intermediario ha provveduto al blocco dello *home banking* in data 11.08.2020 per "*operazione/flusso anomalo*";
- che agli inizi del settembre 2020 si accorgeva che, sempre nella giornata dell'11.08.2020, era stata compiuta un'ulteriore operazione di € 390,00, questa volta tramite la carta di credito, parimenti disconosciuta.

Afferma che le transazioni sono avvenute senza alcuna richiesta né comunicazione di PIN/credenziali e senza alcuna autenticazione forte sostenendo che le stesse "*non sono state effettuate con l'accesso tramite credenziali, avendo sia l'home banking che la carta di credito PIN che nulla hanno a che vedere con le credenziali di accesso, peraltro anch'esse mai inserite*".

Lamenta la negligenza dell'intermediario per non aver bloccato preventivamente i movimenti anomali "*da esso stesso identificati come tali*".

Ritiene che la truffa informatica occorsa sia identificabile come "*home banking e phishing/man-in-thebrowser*" richiamando l'obbligo per gli intermediari di adottare accorgimenti adeguati per prevenire l'illecita captazione di dati attraverso il *phishing*, onde evitare accessi non autorizzati.

Afferma che *"[q]ualora si verifichi un accesso non autorizzato o l'impiego dei dati raccolti per finalità non conformi alla legge, il gestore risponde ex art. 2050 c.c.*" trattandosi di responsabilità oggettiva "*aggravata*" e che pertanto il prestatore del servizio, per andare esente da responsabilità, non deve solo dimostrare di aver adottato tutte le misure idonee ad evitare il danno sofferto, ma fornire altresì la prova positiva di una causa esterna.

Sostiene che, nel caso di specie, l'intermediario non ha adottato la diligenza professionale richiesta, né dimostrato l'adeguatezza dei presidi di sicurezza predisposti; in particolare non ha dimostrato che le operazioni sono state eseguite con un sistema dinamico di autenticazione né la presenza di un servizio di *SMS Alert*. Inoltre non ha sospeso in via precauzionale la seconda transazione sospetta.

Contesta la presunzione di negligenza a suo carico che l'intermediario vorrebbe attribuirgli.

Chiede pertanto il rimborso della somma di € 780,00.

Con le controdeduzioni l'intermediario rileva che nella denuncia all'A.G. e successiva integrazione effettuate dal ricorrente vengono descritte solo in parte le modalità con cui è stata perpetrata la frode.

Evidenzia che il ricorrente riferisce nella denuncia all'A.G. di aver "*distrattamente*" inserito i propri dati identificativi nonché i dati relativi al conto corrente e alle sue carte di credito e debito a seguito di una *email* di *phishing*, ma che, tuttavia, non riferisce di aver ricevuto gli *sms* da esso inviatigli, come quello con il codice riservato per l'attivazione del *mobile token* o quelli con cui veniva avvisato dell'avvenuta configurazione dell'*App* e digitalizzazione delle due carte di pagamento.

Riporta il testo e l'orario dei messaggi che ha inviato al cellulare del cliente, rilevando che gli stessi sono stati trasmessi in data 11.08.2020 (tra le ore 21.58 e le ore 22:03), mentre

l'asserita frode è stata portata a compimento soltanto alle ore 20:40 (pagamento POS tramite carta bancomat) e 20:41 del giorno successivo (pagamento POS tramite carta di credito).

Precisa che nella specie il codice OTP, per l'attivazione del *mobile token*, è stato inviato al cliente via *sms* in data 11.08.2020 alle ore 21:58:53.

Evidenzia che l'attivazione del *Mobile Token* è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza, "*rivelate dal ricorrente con tutta probabilità a terzi non autorizzati, stante la colpevole distrazione ammessa*", dell'*home banking* e del codice OTP.

Osserva che il ricorrente non solo ha fornito i dati del conto corrente e delle carte ma non si è "*neanche allarmato quando ha ricevuto gli SMS sulla sua utenza telefonica riguardanti servizi e App di cui non aveva lui stesso richiesto l'attivazione*".

Sintetizza quindi il processo di digitalizzazione delle carte con l'*App "A****Pay"* evidenziando che a tal fine è necessario inserire le credenziali per l'accesso allo *home banking* e, per completare il processo, l'OTP. Una volta installata l'*App*, la stessa conterrà le carte associate al conto corrente del titolare che possono, quindi, essere utilizzate per effettuare pagamenti direttamente tramite la *App* medesima.

Riferisce che dalle verifiche effettuate è risultato che entrambe le carte sono state oggetto di collegamento con l'*App A****Pay* e che nell'occasione ha inviato i relativi messaggi *sms* sull'utenza telefonica del cliente alle 22:03:04 dell'11.08.2020.

Precisa che le operazioni disconosciute sono state poi eseguite con la lettura delle carte digitalizzate su *Wallet* "A**** Pay", secondo le modalità previste in fase di autenticazione della transazione e cioè avvicinando il dispositivo al POS *contactless* abilitato e confermando la transazione tramite TouchID o FaceID.

Precisa che tale modalità di autenticazione è indicata nei *log* per la carta bancomat dal "*codice 022*", laddove la settima cifra "*lettera L*" indica la modalità "*contactless*" e per la carta di credito dal codice "*POS ENTRY MODE = 07*".

Fornisce quindi una legenda dei codici contenuti nei *Log*.

Osserva che il ricorrente avrebbe avuto il tempo per bloccare sia le carte che l'*home banking*, considerato che la digitalizzazione delle carte gli è stata notificata via *sms* alle ore 22:03 dell'11.08.2020, mentre le operazioni sono state eseguite alle ore 20:40 e 20:41 del giorno successivo.

Riferisce che le due carte sono state bloccate cautelativamente in data 14.08.2020 alle ore 08:35 (carta bancomat) e alle ore 15:54 (carta di credito).

Ritiene molto plausibile che soggetti terzi abbiano proceduto alla digitalizzazione delle carte del ricorrente, dopo aver attivato il *mobile token*, in totale autonomia e solo grazie al coinvolgimento del ricorrente.

Evidenzia come "*il frodatore, a conoscenza dei dati necessari a perpetrare la frode in esame, quali il numero della carta di credito e del codice CVV nonché del numero della carta di debito comunicati dal ricorrente in seguito alla email di phishing, come ha dichiarato lui stesso in denuncia, sia riuscito ad acquisire il codice necessario per completare la digitalizzazione della carta di credito e di debito*" inviato dall'intermediario al telefono del ricorrente.

Aggiunge che, una volta effettuata la digitalizzazione della carta sul proprio cellulare, il frodatore è in grado di autorizzare la transazione con la carta mediante la propria impronta digitale o mediante un PIN da lui stesso stabilito.

Ritiene pertanto di aver posto in essere tutte le misure di sicurezza idonee e che "*la frode è stata resa possibile esclusivamente dalla conoscenza, in capo ai presunti frodatori, delle credenziali di accesso all'home banking, senza le quali non sarebbero stati in grado di scaricare il Mobile Token, accedere alla App e quindi digitalizzare le carte e, con esse, eseguire le operazioni oggetto del ricorso*".

Sostiene inoltre di essere molto attento nell'informare la propria clientela sulle possibili frodi.

Ritiene che il ricorrente abbia adottato una condotta omissiva e reticente nel descrivere i fatti.

Richiama la decisione del Collegio di Roma n.1386/20 nonché altre pronunce dei Collegi ABF.

Chiede pertanto che il ricorso sia respinto, in quanto le operazioni disconosciute sono state regolarmente autenticate, registrate e contabilizzate, ritenendo la frode ascrivibile alla grave negligenza del ricorrente nella custodia delle credenziali di sicurezza.

In sede di repliche, il ricorrente contesta le deduzioni dell'intermediario.

In particolare, afferma di non aver mai riferito di aver "*distrattamente*" inserito i dati del conto corrente e delle carte ma di aver provveduto "*ad una conferma/aggiornamento, dei dati identificativi personali della carta (es. nome e cognome ecc…)*".

Precisa, inoltre, che il termine "*distrattamente*" utilizzato nella denuncia all'A.G. "*va contestualizzato alla circostanza di fatto, dettata dall'effettiva presa di coscienza della frode subita, ma … non rappresenta l'elemento psicologico soggettivo, presente il giorno stesso, in cui effettuava il mero click nella mail*".

Sostiene altresì di non aver mai ricevuto i messaggi indicati dall'intermediario, "*oltre al fatto che, laddove fossero stati ricevuti, considerata la buona fede …, sarebbero stati successivi al click da lui effettuato e quindi rappresenterebbero la naturale conseguenza di quanto aggiornato e richiestogli via mail. Quindi a nulla servono, né sarebbero serviti, gli indicati sms che, non fanno altro, che rafforzare quanto precedentemente fatto/eseguito, aumentando il convincimento della veridicità nonché lealtà della richiesta, pervenuta dalla mail*".

Ritiene che la condotta negligente dell'intermediario emerga anche dalla circostanza che il blocco delle carte in questione è stato effettuato tre giorni dopo il secondo pagamento fraudolento.

Lamenta di non aver mai ricevuto la risposta al reclamo allegata alle controdeduzioni, stante l'erronea indicazione dell'indirizzo *mail* del destinatario.

Chiede al riguardo "*l'immediata estromissione*" dal fascicolo del suddetto allegato "*e l'applicazione della relativa sanzione/penale, inerente la mancata risposta al reclamo*".

Ribadisce quindi quanto affermato nel ricorso sulla responsabilità dell'intermediario.

Sottolinea inoltre la natura "*alquanto strana ed inusuale*" delle transazioni, con beneficiario estero, in relazione alle proprie abitudini.

Contesta la presunzione di negligenza a suo carico che l'intermediario vorrebbe attribuirgli nonché quanto sostenuto da controparte circa la vaghezza del ricorso.

Conclude ribadendo le istanze formulate nel ricorso chiedendo inoltre la rifusione delle spese di assistenza professionale e *l'estromissione dell'allegato n.2 del fascicolo dell'intermediario e successiva condanna del**l'**[intermediario], al pagamento dell'indennizzo per la mancata risposta al reclamo*".

In sede di controrepliche, l'intermediario conferma quanto affermato nelle controdeduzioni, richiamando a supporto alcune pronunce dei Collegi territoriali.

Nella seduta del 22 luglio 2021 il Collegio di Bari, territorialmente competente a pronunciarsi sul ricorso in questione, osserva che la complessità del tema riguardante la prova di autenticazione che l'intermediario deve produrre con riguardo alle operazioni di pagamento effettuate tramite *mobile wallet* e il diverso orientamento seguito al riguardo dai Collegi territoriali rendono opportuna la rimessione della decisione della controversia al Collegio di Coordinamento.

Con ordinanza n. 18412/21 del 4 agosto 2021 il Collegio di Bari ha pertanto rimesso la decisione della presente controversia a questo Collegio.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Decisione N. 21285 del 11 ottobre 2021

DIRITTO

1. La controversia attiene alla responsabilità per l'esecuzione fraudolenta di due operazioni di pagamento effettuate attraverso l'utilizzo del *mobile wallet A***Pay*.

2. Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218, che ha recepito la direttiva 2015/2366/UE relativa ai servizi di pagamento nel mercato interno (c.d. PSD2) e del Regolamento (UE) 2018/389 del 27 novembre 2017 (RTS) che integra la PSD2 per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli *standard* aperti di comunicazione comuni e sicuri.

In particolare, l'articolo 10, commi 1 e 2, del citato decreto dispone che "1. *Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti. 1-bis (omissis). 2. Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo della colpa grave dell'utente*".

L'art. 10-*bis*, comma 1, del d.lgs. n.11/2010 dispone che in conformità all'articolo 98 della PSD2 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, "*i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*".

L'art. 1, lettera q), del d.lgs. n.11/2010 ("Definizioni") definisce per *"autenticazione: la procedura che consente al prestatore di servizi di pagamento di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di*

pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore".

La definizione di autenticazione forte (SCA) è fornita dalla successiva lettera *q-bis)* ove si specifica che per autenticazione forte del cliente si intende: "*un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente) che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione*".

Tale definizione riprende il disposto dell'art. 4 del Regolamento 2018/389 ove si prevede che "*Se i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente conformemente all'articolo 97, paragrafo 1, della direttiva (UE) 2015/2366, l'autenticazione si basa su due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza e comporta la generazione di un codice di autenticazione*".

L'art. 12, comma 2-*bis*, del d.lgs. n. 11/2010, stabilisce che «*salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente (…)*».

L'art. 5, comma 6, del D. Lgs. 218/2017 prevede che le misure di sicurezza, di cui all'art. 10-*bis*, così come declinate dalle norme tecniche di regolamentazione, di autenticazione e comunicazione, si applicano decorsi diciotto mesi dalla data di entrata in vigore di tali norme.

Tali norme sono contenute nel Regolamento n. 2018/389, le cui disposizioni si applicano a decorrere dal 14 settembre 2019 (art. 38, paragrafo 2) e cioè diciotto mesi dopo l'entrata in vigore del Regolamento.

Il 21 giugno 2019 l'Autorità Bancaria Europea (EBA) ha emanato la "*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*", con cui ha precisato, ai fini dell'implementazione del suddetto Regolamento, quali elementi costituiscano o meno, allo stato attuale della tecnologia, fattori di autenticazione forte all'interno delle categorie della conoscenza, del possesso e dell'inerenza.

Il quadro normativo sopra richiamato va necessariamente integrato, ai fini di una compiuta valutazione della questione in esame, dai pertinenti interventi dell'Autorità Bancaria Europea, in termini di *Opinion* (in particolare la suddetta Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2), di Linee guida

(in particolare le *Guidelines on outsourcing arrangements*), di chiarimenti forniti in risposta a quesiti (Q&A).

3. Venendo al merito del ricorso, si rileva che il ricorrente ha dichiarato, in sede di denuncia all'A.G., di essersi avveduto alle 20:40 circa del 12.08.2020 di un'operazione da lui disconosciuta, eseguita con la sua carta bancomat, e di essere stato avvisato dall'Ufficio Frode dell'intermediario convenuto, alle ore 16:00 del 13.08.2020, dell'avvenuta truffa.

Nella successiva denuncia all'A.G. il ricorrente afferma di aver ricevuto in data 11.08.2020 una *mail* (non depositata in atti) con cui si chiedeva "*l'aggiornamento dei [suoi] dati identificativi, nonché di quelli della … carta di credito e conto corrente cosa che … distrattamente effettuav[a]*".

Il 12.08.2020 il ricorrente si avvedeva del blocco del servizio di *home banking* e, successivamente, di una seconda operazione da lui disconosciuta, effettuata con la sua carta di credito.

Le operazioni contestate consistono in due pagamenti effettuati il 12.08.2020 rispettivamente: i) con la carta bancomat, alle ore 20:40 del 12.08.2020, di € 390,00; ii) con la carta di credito, alle ore 20:41 del 12.08.2020, di € 390,00.

In sede di repliche alle controdeduzioni il ricorrente afferma che, a seguito della *mail* ricevuta", ha "*solo provveduto ad una conferma/aggiornamento dei dati identificativi personali della carta*".

Le carte risultano bloccate in data 14.08.2020.

4. Le operazioni in questione sono state effettuate tramite *mobile wallet*.

E' opportuno pertanto precisare preliminarmente, come fa l'ordinanza di rimessione, le modalità con cui si perviene all'inserimento della propria carta di pagamento nel *wallet* e al successivo utilizzo della stessa per effettuare operazioni di pagamento.

Una prima fase, detta anche di *tokenizzazione*, consiste, nella registrazione della carta nel *wallet*.

Gli *standard* dei *wallet provider* consentono ad oggi due modalità di *tokenizzazione* della carta: i) dall'*App* di *mobile banking*: in questo caso i dati della carta sono già disponibili e l'utente può dare il comando "*aggiungi carta al wallet*"; ii) dall'interno del *wallet*: in questo caso i dati della carta sono catturati dalla fotocamera o con *input* manuale.

Trattandosi di una operazione condotta da remoto che può comportare frodi e altri abusi, la registrazione della carta nel *mobile wallet* richiede l'autorizzazione forte (SCA), secondo

quanto previsto dall'art. 10-*bis*, comma 1, lett. c), del d.lgs. n.11/2010 (art. 97, paragrafo 1, della PSD2), come puntualizzato da EBA nella QA 2019_4910.

Questa SCA è gestita direttamente dall'emittente, che ne può scegliere tipologia e caratteristiche nell'ambito di quelle supportate dal *wallet provider* e dal circuito di riferimento.

Una seconda fase consiste nell'utilizzo del *mobile wallet* per effettuare il pagamento elettronico scegliendo la carta di pagamento che si vuole utilizzare.

L'operazione – salve le esenzioni sulla base delle previsioni dello RTS (artt. 10-18) – richiede l'autenticazione del cliente con la SCA che, a differenza delle carte fisiche, avviene interamente sullo *smartphone*.

Uno degli elementi necessari per la SCA è costituito dal possesso dello *smartphone* con *App e Token* a bordo; l'altro è uno a scelta tra un elemento di inerenza (ad esempio un fattore biometrico quale il *FaceID* o il *TouchID*) e un elemento di conoscenza (ad esempio un codice statico).

Al momento del pagamento la combinazione di questi due fattori genera il codice univoco di autenticazione (cfr. RTS, art. 4) che viene inviato al POS. Le transazioni sono pertanto proposte al POS dal *wallet* come "*gia autenticate*" e perciò il POS non chiede il PIN.

Nei pagamenti eseguiti tramite *mobile wallet* l'operatività dello strumento, compresa l'autenticazione forte, viene gestita tramite i servizi tecnici offerti dal *wallet provider* all'emittente sulla base dell'accordo contrattuale fra l'emittente lo strumento di pagamento e il gestore del *wallet*. Le credenziali dell'utente sono pertanto gestite dal *wallet provider*.

5. Come sopra indicato qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Inoltre l'autenticazione forte è richiesta non solo quando l'utente effettua un'operazione di pagamento elettronico, ma anche allorché effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi (oltreché quando accede al suo conto di pagamento *online*).

6. Quanto alla digitalizzazione delle carte in questione l'intermediario dichiara: i) di ritenere "*molto plausibile che soggetti terzi abbiano proceduto alla digitalizzazione delle carte del ricorrente, dopo aver attivato il mobile token, in totale autonomia …*"; ii) che la

digitalizzazione richiede l'inserimento di "*tutte le credenziali necessarie per l'accesso alla home banking" e "dell'OTP per completare il processo".*

L'intermediario riferisce in merito di aver rilevato una richiesta di attivazione del *mobile token* collegato all'*App* della banca riconducibile al ricorrente e di aver inviato un *sms* al cellulare di quest'ultimo, di cui riporta il testo e il *report*, con cui comunicava il codice riservato per l'attivazione del *mobile token,* del seguente tenore: "*Stai attivando il Mobile Token. Ricordati che il personale (…) non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato*".

Seguiva un *sms,* a cura del comparto dell'intermediario NFC/Wallet/…, di cui riporta il testo e il *report*, con il quale il ricorrente veniva avvisato dell'avvenuta configurazione dell'*App* della banca, del seguente tenore: "*il 11/08/2020 h. 22:03 hai configurato l'App (…). Se non hai eseguito questa operazione, chiama il n. …*".

L'intermediario riferisce inoltre di aver inviato al cliente due ulteriori *sms* per avvisarlo dell'avvenuta digitalizzazione delle sue carte di debito e di credito sull'*App A***Pay*: i) un primo *sms* (ore 22:03:29) con il seguente testo, che riporta nelle controdeduzioni: "*La tua carta di credito ***1433 è stata abbinata a A*** Pay. Da ora puoi pagare quando vuoi dove vedi il simbolo contactless o il logo A*** Pay*"; ii) un secondo *sms* (ore 22:03:44) con il seguente testo, che riporta nelle controdeduzioni: "*La tua carta di debito ***4843 è stata abbinata a A*** Pay. Da ora puoi pagare quando vuoi dove vedi il simbolo contactless o il logo A*** Pay*".

Non produce ulteriori elementi documentali al riguardo, in ispecie i pertinenti *log* informatici.

Dagli elementi forniti da parte resistente, può evincersi che la digitalizzazione delle carte in questione è stata quindi preceduta dall'installazione dell'*App* bancaria previo invio del codice OTP necessario per l'attivazione del *mobile token*.

7. Con la Q&A 2019_4910 l'EBA ha confermato che "*Adding a payment card to a digital wallet is an action which may imply a risk of fraud or other abuses and thus would require the application of SCA. This means that … the payer would need to apply SCA for accessing its payment account via its mobile application and apply a second SCA when adding the payment card to a digital wallet*".

L'abbinamento di una carta di pagamento a un *digital wallet* rientra quindi nelle fattispecie di cui all'art. 10-bis,comma 1, lett. c), d.lgs. n.11/2010 e richiede quindi la SCA.

Peraltro il prestatore di servizi di pagamento è tenuto ad applicare la SCA, ai sensi all'art. 10-bis,comma1, lett. c), d.lgs. n.11/2010, anche alla fase preliminare di attivazione del *mobile token*, propedeutica a quella della digitalizzazione.

Pertanto anche ove si ritenga provat**o**, sulla base degli *sms* prodotti, che l'attivazione del *mobile token* è stata effettuata in conformità ai requisiti di autenticazione forte, non pare possibile giungere alla stessa conclusione per la fase di digitalizzazione, in mancanza dì evidenze circa l'utilizzo, a tal fine, delle credenziali per l'accesso *all'home banking* e di un apposito OTP.

Né soccorre la probabile circostanza, visto il breve tempo intercorso fra il primo *sms* (*alert* sull'attivazione del *mobile token*) e l'ultimo (comunicazione dell'avvenuta digitalizzazione delle carte) che l'attivazione del *mobile token* e la digitalizzazione delle carte siano avvenute nel corso della stessa sessione di *home banking* poiché anche in tal caso, come ha puntualizzato l'EBA in più occasioni (Q&A 2019_4910, Q&A 2019_4783; Q&A 2018_4141) ogni fase richiede una specifica autenticazione forte, se del caso riutilizzando le credenziali di accesso.

Inoltre l'intermediario dichiara nelle controdeduzioni che "*Il frodatore, a conoscenza dei dati necessari a perpetrare la frode in esame, quali il numero della carta di credito e del codice CVV nonché del numero della carta di debito comunicati dal ricorrente in seguito alla email di phishing, come ha dichiarato lui stesso in denuncia, sia riuscito ad acquisire il codice necessario per completare la digitalizzazione della carta di credito e di debito*".

Non è chiaro se i dati delle carte abbiano rappresentato il necessario oggetto del processo tecnico di digitalizzazione ovvero dei fattori di autenticazione (peraltro in contraddizione con quanto affermato dallo stesso intermediario, secondo cui sono richieste a tal fine *"le credenziali necessarie per l'accesso alla home banking" e l'OTP*).

Se per l'autenticazione della digitalizzazione delle carte fossero stati utilizzati i dati statici delle stesse tale operazione non risulterebbe, anche per questo profilo, effettuata secondo i requisiti richiesti per la SCA.

Infatti, come chiarito dall'EBA con la "*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*" del 21 giugno 2019, i dati presenti sulla carta di pagamento non sono elementi né di conoscenza, né di possesso (né tantomeno di inerenza), trattandosi di elementi potenzialmente catturabili o accessibili da soggetti terzi, e non costituiscono quindi un fattore di autenticazione forte.

8. In definitiva non risulta che l'intermediario abbia, nel caso di specie, fornito prova dell'autenticazione forte della digitalizzazione delle carte in questione.

In mancanza di tal prova l'intermediario sopporta integralmente le conseguenze delle operazioni disconosciute.

Risulta pertanto superfluo verificare eventuali profili di responsabilità ascrivibili al ricorrente, in relazione alla condotta tenuta nella vicenda.

Va rigettata la richiesta di rifusione delle spese di assistenza professionale essendo stata formulata per la prima volta in sede di reclamo e, comunque, non avendo il ricorrente prodotto la fattura dimostrativa del pregiudizio che assume aver sopportato.

9. Ciò posto, benché la questione sollevata dall'ordinanza di rimessione non sia strettamente funzionale alla decisione del caso di specie, il Collegio ritiene che ne sia opportuna la trattazione viste le divergenze interpretative registrate a riguardo fra i Collegi territoriali.

Come più sopra indicato, il punto critico sollevato dall'ordinanza riguarda la prova dell'autenticazione forte dell'utente in ordine agli atti dispositivi dei due pagamenti contestati, compiuti attraverso l'utilizzo del *wallet A***Pay*. L'ordinanza sottolinea al riguardo che va considerato che nei pagamenti eseguiti tramite *mobile wallet* l'operatività dello strumento, compresa la SCA, viene gestita tramite i servizi tecnici offerti dal *wallet provider* all'emittente, sulla base di un accordo contrattuale; in particolare, le credenziali dell'utente sono gestite dal *wallet provider*.

In proposito, l'intermediario afferma che le operazioni di pagamento disconosciute sono state disposte regolarmente, il 12.08.2020, con sistema dinamico di autenticazione a due fattori: i) un fattore di possesso, rappresentato dall'utilizzo dello *smartphone* con l'*App A*** Pay* che contiene le carte associate e che viene accostato al POS, fungendo così da *(mobile) token*; ii) un fattore di inerenza, attraverso l'impronta digitale o la geometria del volto rilevate per mezzo della funzione "*TouchID*" o "*FaceID*" dello *smartphone*.

Si osserva al riguardo che l'utilizzo dello *smartphone* con l'*A***Pay* costituisce un fattore di possesso, secondo quanto indicato dall'EBA nella citata *Opinion* del 21 giugno 2019, in cui si chiarisce che i) "*possession does not solely refer to physical possession but may refer to something that is not physical, such an app* (paragrafo 24)*;* ii) *EBA is of the view that approaches relying on mobile apps … may also be evidence of possession provided that they include a device–binding process that ensures a unique connection between the PSU's app … and the device* (paragrafo 26)".

Peraltro nella Q&A 2019_4827 l'EBA ha specificato che la carta digitalizzata può rientrare fra gli elementi di possesso contemplati dalla SCA se il prestatore di servizi di pagamento è direttamente o indirettamente coinvolto nel processo di rilascio del *token*, in modo da

consentire la verifica dell'identità dell'utilizzatore e l'associazione del *token* a un dispositivo affidabile.

L'ulteriore fattore su cui si è basata l'autenticazione forte delle operazioni di pagamento in questione è costituito, secondo quanto riferito dall'intermediario, dalla funzione "*TouchID*" o "*FaceID*" dello *smartphone.* Si tratta di fattori di inerenza (*fingerprint scanning* e *face geometry*) ritenuti conformi alla SCA dalla suddetta *Opinion* dell'EBA.

L'intermediario produce gli *screenshot* delle operazioni contestate da cui afferma evincersi che le stesse sono state effettuate "*ponendo le carte digitalizzate a contatto con il POS tramite A***Pay*".

Per l'operazione effettuata con la carta bancomat la documentazione prodotta indica, secondo la *legenda* fornita dall'intermediario, che l'operazione è stata effettuata alle ore 20:40:45 del 12.08.2020 in modalità *contactless* e riporta il PAN che identifica la tessera, oltre all'importo dell'operazione, al codice del POS presso cui la stessa è stata effettuata e i dati dell'esercente.

Per l'operazione effettuata con la carta di credito la documentazione prodotta riporta il numero della carta, che l'operazione è stata effettuata alle ore 20:41 del 12.08.2020 in modalità *contactless* (*PosEntrymode=07*), che è stata autorizzata tramite wallet A***Pay (PSD0207=103), il codice di autorizzazione.

Se quindi potrebbe ritenersi fornita la prova della sussistenza del fattore di autenticazione forte "possesso" (qualora fosse stata correttamente *tokenizzata* la carta), considerato che le operazioni di pagamento risultano effettuate in modalità *contactless* con le carte digitalizzate in questione, dalla documentazione prodotta non è rinvenibile evidenza dell'avvenuta applicazione del fattore di inerenza che l'intermediario riconduce all'attivazione della funzione "*TouchID*" o "*FaceID*" dello *smartphone.*

10. L'ordinanza di rimessione rileva come l'orientamento dei Collegi in ordine alla prova di autenticazione forte delle operazioni di pagamento in fattispecie di utilizzo del digital *wallet* si presenta come non univoco. Sottolinea che l'intera procedura di pagamento non può sfuggire ad un'analisi del caso concreto al fine di valutare la correttezza dell'operato dell'intermediario (oltreché l'eventuale ricorrenza di una fattispecie di colpa grave del ricorrente).

Cita la decisione n. 8831/2021 dello stesso Collegio remittente, che in una fattispecie riconducibile a quella in esame, ha accolto la domanda del ricorrente, rilevando che parte resistente espone "*Quanto alle singole operazioni, … che la "autorizzazione non è tracciata nei (suoi) log", rimanendo propria del Wallet Provider". Fa presente, in ogni caso,*

che su tale wallet ogni transazione è autenticata utilizzando un elemento di possesso (il "token" di pagamento) e un elemento di inerenza (riconoscimento facciale/impronta digitale) o di conoscenza (PIN)".

La stessa decisione puntualizza che "*Lo stesso intermediario, peraltro, nulla prova con riferimento alla regolare autenticazione delle singole operazioni, limitandosi ad affermare che l'autorizzazione non sarebbe tracciata nei suoi log, rimanendo propria del Wallet Provider*".

Cita inoltre la decisione del Collegio di Roma, n. 6922/2021 che in un caso molto simile a quello di specie, peraltro nei confronti del medesimo intermediario, ha ritenuto che "*Nel corso del procedimento l'intermediario ha, altresì, provato – producendo i log dei singoli pagamenti – che le operazioni disconosciute sono state disposte regolarmente con sistema dinamico di autenticazione a due fattori, peraltro distinti da quelli impiegati in fase di accesso all'home banking nonché in fase di digitalizzazione degli strumenti di pagamento: i. un fattore di possesso, rappresentato dall'utilizzo dello smartphone con l'App A*** Pay che contiene già le carte associate e che viene accostato al POS, fungendo così da (mobile) token; ii. un fattore di inerenza, attraverso l'impronta digitale o la geometria del volto rilevate per mezzo della funzione "TouchID" o "FaceID" dello smartphone*". Nel medesimo senso, più di recente, Collegio di Roma, dec. n. 13119/2021.

Si osserva che in entrambi i casi oggetto delle decisioni del Collegio di Roma, l'intermediario produce documentazione da cui si evince che le operazioni contestate sono state effettuate in modalità *contactless*, mentre non è fornita evidenza in merito al fattore di inerenza.

Cita altresì la decisione n. 9325/2021 con cui il Collegio di Milano osserva che "S*i tratta di operazioni eseguite a seguito dell'attivazione da parte dei truffatori del canale di pagamento A***Pay. Alla luce di quanto finora esposto deve affermarsi la colpa grave della cliente utile a consentire la realizzazione delle operazioni fraudolente".* Nel caso di specie dalla documentazione prodotta dall'intermediario si evince che l'operazione contestata è stata effettuata, tramite carta digitalizzata su *Wallet A***Pay,* su sito sicuro, come attestato dal codice utilizzato nel circuito VISA indicato, che richiede un'autenticazione forte del cliente.

La decisione conclude riconoscendo un concorso di colpa dell'intermediario pari al 20%, in quanto, nel caso esaminato erano state effettuate tre operazioni presso il medesimo esercente, circostanza ritenuta rilevante quale indizio di frode, che avrebbe dovuto indurre l'intermediario ad adottare ulteriori misure precauzionali.

Differente, invece, la posizione assunta dal Collegio di Palermo con la decisione n. 13163/2021), il quale rileva che: " … *l'intermediario è tenuto comunque a provare che la doppia autenticazione sia prevista anche al momento della finalizzazione del pagamento (cfr. Coll. Palermo, n.14147/2020). … Senonché al fine di provare le predette circostanze [l'intermediario] si limita a produrre i log informatici delle operazioni, da cui non risulta possibile rilevare l'avvenuta autenticazione tramite TouchID o FaceID. Neppure con riguardo alla fase in parola, dunque, può affermarsi che l'intermediario abbia assolto all'onere probatorio su di esso gravante di avere adottato modalità di autenticazione dell'operazione conformi al sistema di strong customer authentication. In definitiva, non avendo l'intermediario dimostrato di aver adottato un sistema di autenticazione forte, né nella fase della digitalizzazione/associazione della carta al wallet, né in quella successiva dell'effettuazione della transazione, non può che affermarsi la sua responsabilità per l'operazione contestata, risultando irrilevante un eventuale concorso di colpa del cliente*".

11. Ciò posto, si osserva che con la Q&A 2018_4047 l'EBA ha chiarito che gli emittenti di una carta di pagamento possono usare la tecnologia fornita da terzi, quale ad esempio il lettore dell'impronta digitale, a supporto della SCA e per assicurare l'adozione di tutte le misure di sicurezza stabilite nel Regolamento 2018/389.

Inoltre i prestatori di servizi di pagamento possono esternalizzare a un terzo l'esecuzione della SCA, nel rispetto dei requisiti previsti dagli "*Orientamenti in tema di esternalizzazione*" a cura dell'EBA.

L'EBA ha peraltro precisato che la responsabilità dell'osservanza delle prescrizioni in tema di SCA non può essere esternalizzata dai prestatori di servizi di pagamento a soggetti terzi e che i prestatori di servizi di pagamento sono pienamente responsabili per la conformità della SCA al Regolamento 2018/389.

Inoltre con la Q&A 2019_4937 l'EBA ha precisato che, benché l'esecuzione di una SCA possa esser affidata a un terzo, ciò non include il pagatore considerato che ai sensi dell'art. 4(29) della PSD2 l'autenticazione è una procedura di verifica dell'identità di un utente di servizi di pagamento e pertanto non può essere gestita dallo stesso.

12. In conclusione in base al quadro normativo sopra delineato, così come corredato dagli interventi dell'EBA, non può che confermarsi che spetta all'intermediario la prova dell'intervenuta autenticazione forte delle operazioni di pagamento nonché, per quanto rileva ulteriormente nel caso di specie, di qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Il fatto che la fase relativa alla disposizione di pagamento tramite carta digitalizzata sia gestita dal *Wallet provider* non esime il prestatore di servizi di pagamento dalla piena responsabilità per quanto attiene all'adozione delle prescritte misure di sicurezza in tale fase e quindi per la conformità delle modalità di autenticazione delle operazioni di pagamento ai requisiti della SCA.

Ciò implica che l'intermediario debba fornire la prova che le operazioni di pagamento siano state disposte con modalità di autenticazione forte, non potendosi ritenere ciò implicito dal fatto che le transazioni risultino autorizzate o comunque dalla sola evidenza che siano state effettuate in modalità *contactless*.

Rammentato che il ricorso va accolto, si enuncia il seguente principio di diritto:

"L'utilizzo di un wallet affidato a un terzo gestore per l'esecuzione di operazioni di pagamento 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".

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e per l'effetto dispone che l'intermediario corrisponda alla parte ricorrente l'importo di € 780,00.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di € 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA