

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) TRAVERSI	Membro di designazione rappresentativa dei clienti

Relatore ELEONORA MIRABELLI

Seduta del 13/01/2026

FATTO

La ricorrente, anche per mezzo della documentazione allegata al ricorso, riferisce che in data 16.7.2024 veniva effettuato, utilizzando la carta di credito emessa dall'intermediario resistente, un acquisto *on line* per un importo pari ad € 1,19. In data 07.08.2024, da una verifica sulle proprie movimentazioni bancarie, si avvedeva che, a detta data, risultavano effettuati altri 29 acquisti sul medesimo sito, il cui totale ammontava inizialmente ad € 3.046,13; provvedeva dunque immediatamente al blocco della carta di credito ed al disconoscimento di dette operazioni, denunciando inoltre l'accaduto ai Carabinieri. In data 23.8.2024 veniva inoltre sporta querela, poi integrata in data 10.9.2024, per denunciare tre ulteriori addebiti, datati 6 agosto 2024, sempre sul medesimo sito, che portavano il totale delle operazioni complessivamente disconosciute a 32, per complessivi € 3.921,76. In data 23 agosto 2024 veniva inviato un reclamo con cui si disconoscevano le suddette operazioni (ad eccezione della prima del 16.7.2024, di importo pari a € 1,19) e veniva rappresentato che per tali operazioni non erano mai stati ricevuti gli avvisi delle operazioni disconosciute, mentre erano stati regolarmente ricevuti gli avvisi relativi alle altre operazioni effettuate con la carta di credito e non disconosciute. L'intermediario riscontrava i vari reclami, continuando a non fornire alcuna prova in ordine alle evidenze informatiche a conferma delle asserite autorizzazioni al pagamento da parte della ricorrente ed è dunque evidente la responsabilità dell'intermediario – che non ha fornito prova in ordine alla corretta autenticazione, registrazione e contabilizzazione delle operazioni - per quanto occorso alla

ricorrente, con conseguente diritto della stessa alla più volte richiesta restituzione dell'importo di € 3.921,76.

In sede di controdeduzioni, l'intermediario eccepisce che la richiesta dei ricorrenti risulta del tutto lacunosa, supportata da documenti incongruenti tra loro, tanto da non consentire nemmeno agli stessi di circostanziare il danno asseritamente subito: infatti, secondo quanto dichiarato nel modulo di disconoscimento il danno ammonta ad € 3.046,13, ma nel reclamo il ricorrente lo quantifica dapprima in € 3.992,95 e successivamente in € 3.921,76. I clienti non hanno mai formalmente disconosciuto le ulteriori tre operazioni eseguite il 06.08.2024 per complessivi € 876,82, le quali non sono dettagliate e comprensibili nemmeno del prodromico reclamo: pertanto, relativamente alle già citate operazioni, il ricorso è da ritenersi inammissibile per mancanza di reclamo. Nel merito, l'intermediario eccepisce che, per accedere ai servizi online della Banca è richiesto l'inserimento simultaneo di password statiche e dinamiche, cioè il codice Titolare (password statica) il codice PIN (password statica) e il codice O-Key (OTP cioè la password dinamica). Una volta collegati al servizio online, per autorizzare le operazioni dispositive è necessario il codice dinamico, OTP il quale viene generato: i) via software dall'APP, per i clienti che hanno attivato O-Key Smart; ii) via SMS (inoltrato sul numero di telefono certificato), per i clienti che hanno attivato O-Key SMS. Con l'utilizzo dell'O-Key Smart, i codici O-Key dinamici per accedere ai servizi di banca online e per autorizzare le operazioni sono generati a seguito della selezione della notifica ricevuta sullo smartphone o tablet su cui è stato attivato O-Key Smart e della digitazione su tale smartphone o tablet del PIN oppure, se abilitati, dell'apposizione dell'impronta digitale o del riconoscimento facciale. Eccepisce inoltre l'intermediario di fornire alla propria clientela ampia informativa sul proprio sito internet dove viene sempre sottolineato di prestare attenzione alle e-mail, sms e telefonate sospette e di diffidare da link che prevedano l'inserimento di password. Nel caso di specie, le transazioni risultano autenticate da app con il codice OTP, previa validazione del PIN e l'esecuzione dell'operazione disconosciuta ha rispettato i requisiti della "Conoscenza" – i codici OTP dinamici sono stati generati a seguito della digitazione del PIN, noto solo al Cliente – e del "Possesso" – tali codici sono stati generati tramite l'APP installata sul device. Inoltre, la Banca ha avvisato tempestivamente la ricorrente, diversamente da quanto dalla stessa rappresentato, dell'accaduto, inviando al suo numero di cellulare certificato un messaggio SMS in concomitanza all'esecuzione di ogni operazione: la presunta mancata ricezione di tali alert non dipende dall'operato della Banca bensì dal gestore telefonico, che ha rifiutato tali messaggi per cause certamente non imputabili alla Banca stessa. Il Collegio di Milano, in una fattispecie simile (decisione nr. 1032/2024) ha rilevato che "presumibilmente che il credito presente sulla SIM prepagata del cliente non era sufficiente al pagamento dell'SMS alert di tipo Premium inviato dall'intermediario", escludendo, dunque, la responsabilità dell'intermediario. Inoltre, la ricorrente in denuncia non ha fornito i minimi elementi utili alla ricostruzione della vicenda, limitandosi a disconoscere genericamente le operazioni, né ha fornito, alcuna allegazione che possa consentire di ricostruire e comprovare la dinamica di un'eventuale frode ed ha autorizzato l'operazione dal proprio device le operazioni oggetto di ricorso, le quali devono quindi qualificarsi come operazioni autorizzate ai sensi dell'art. 5, commi 1 e 2, D.lgs. 11/2010, e non risultano quindi sottoposte al regime di speciale protezione e di altrettanto speciale favor probatorio previsto dal già citato D.lgs. Infine, stante il lasso di tempo intercorso dalla data delle prime operazioni disconosciute (16.07.2024) alla data dell'ultima operazione disconosciuta (06.08.2024), se la cliente si fosse attivata tempestivamente per richiedere chiarimenti alla Banca su quanto accaduto, la Banca avrebbe senz'altro potuto impedire l'esecuzione delle operazioni disconosciute. Chiede dunque l'intermediario il rigetto del ricorso in quanto infondato in fatto ed in diritto.

In sede di repliche, parte ricorrente osserva di aver puntualmente quantificato il danno patito in € 3.921,76, valore dato dalla differenza tra il valore delle transazioni avvenute sul sito S*** (€ 3.922,95) e

l'unica transazione effettivamente autorizzata (€ 1,19 in data 16.7.2024), importo che si può desumere anche dalla corrispondenza intercorsa con la banca. A seguito del deposito delle controdeduzioni da parte dell'intermediario, la ricorrente ha sottoposto la documentazione ad esse allegata alla verifica del tecnico informatico, dalla cui relazione risulta che la banca non ha adempiuto all'onere probatorio previsto dall'art. 10 D.Lgs 11/2010 e che non vi è stata alcuna colpa grave nella condotta della ricorrente, come al contrario sostenuto dall'intermediario, essendo infatti altamente probabile che la stessa sia stata vittima di una frode informatica del tipo card-not-present (CNP). Vi sono numerosi elementi che indicano che le transazioni di cui si discute non siano state compiute ed autorizzate dalla ricorrente, ossia: 1) variabilità degli importi; 2) identità del beneficiario per tutte le transazioni sconosciute; 3) il fatto che molte operazioni risultano effettuate in orari notturni o atipici per un utente retail; 4) la presenza di transazioni ravvicinate il che suggerisce un attacco automatizzato per testare limiti e massimizzare il prelievo. Nella denuncia e nelle successive del 23.8.2024 e 10.9.2024 la ricorrente ha fornito ogni elemento utile per la ricostruzione dei fatti, mentre è stato l'intermediario a non fornire, nonostante le reiterate richieste, la documentazione necessaria per le verifiche tecniche, resesi possibili solo dopo il deposito delle controdeduzioni. Nel caso di specie, risulta, tra le altre, la sussistenza dell'indice di anomalia di cui all'art. 8, lett. a, punto 2, D.M. 112/2007: tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita.

L'intermediario, a sua volta, reitera le proprie eccezioni ed insiste per il rigetto del ricorso.

DIRITTO

In via preliminare, il Collegio deve esaminare l'eccezione di inammissibilità sollevata dall'intermediario, il quale ritiene che il ricorso sia generico ed indeterminato, in quanto non sarebbero individuate con chiarezza le operazioni contestate, posto che differirebbero gli importi indicati nel modulo di disconoscimento e nei vari reclami. Eccepisce, inoltre, una parziale difformità tra reclamo e ricorso, in quanto i clienti non avrebbero mai formalmente disconosciuto le ulteriori tre operazioni eseguite il 06.08.2024 per complessivi € 876,82, oggetto del ricorso.

A questo riguardo, il Collegio osserva che nel modulo di disconoscimento vengono indicati 30 addebiti (ivi compreso quello di 1,19 euro, in realtà non sconosciuto), per un totale di 3.046,13 euro. Nei reclami del 04/10/2024 e del 28/11/2024, invece, pur senza indicazione specifica delle operazioni sconosciute, vi è il riferimento a 32 addebiti presenti nel ricorso; nel primo reclamo, il totale viene dapprima indicato in 3.992,95 euro ma la richiesta di rimborso ammonta ad 3.921,76 euro. Ritiene dunque il Collegio che l'eccezione di inammissibilità possa dirsi superata alla luce del fatto che l'intermediario è stato messo a conoscenza del totale delle operazioni contestate, pur non avendo avuto contezza del dettaglio di ogni singolo pagamento.

Ciò premesso, si passa all'esame nel merito delle contestazioni sollevate dalla ricorrente consistenti, dunque, nell'esecuzione fraudolenta da parte di terzi malfattori di n. 32 operazioni di pagamento *on line* verso lo stesso beneficiario, per l'importo complessivo di euro 3.921,76.

Il Collegio rileva che le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la

direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Per consolidato orientamento dei Collegi ABF, a fronte del disconoscimento delle operazioni da parte del cliente, è onere dell'intermediario provare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata, ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010 che così statuisce: "Qualora l'utilizzatore 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". In mancanza di tale prova, dunque, l'intermediario sopporta – in ogni caso – integralmente, le conseguenze delle operazioni disconosciute.

Con riguardo alla modalità di autenticazione delle operazioni, l'art. 10 bis del medesimo D.Lgs. n. 11/2010 prevede: "Conformemente all'articolo 98 della direttiva (UE) 2015/2366 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 bis del medesimo decreto chiarisce, conformemente alla suddetta direttiva, che la c.d. autenticazione forte consiste in "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". Sul punto, è intervenuta l'EBA con la "Opinion" del 21 giugno 2019 (richiamata espressamente dal Regolamento UE/2018/389 del 27.11.2017), nella quale sono stati passati in rassegna alcuni dei più comuni sistemi di autenticazione predisposti dagli intermediari per valutare se possano o meno annoverarsi tra i presidi di autenticazione forte.

Occorre dunque verificare se, nel caso di specie, le operazioni contestate siano state autenticate mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. "autenticazione forte".

A questo riguardo, si osserva che, avendo il cliente previamente installato l'app sul device, l'intermediario ha fornito prova che le operazioni sono state autorizzate previa notifica push in app (fattore di possesso) e mediante un codice OTP ottenuto previa digitazione del codice pin (fattore di conoscenza). (Si fa presente, che, a fronte di analoga documentazione, codesto Collegio ha ritenuto raggiunta la prova della SCA, *cfr.* da ultimo Collegio di Bologna decisione n. 4785/25).

Si ritiene dunque che l'intermediario abbia fornito la prova che tutte le operazioni sono state correttamente registrate, contabilizzate ed autorizzate.

Come però previsto dall'art. 10, comma 2, del d.lgs. n. 11/2010 "Quando l'utilizzatore 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'utilizzatore 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".

Giacché, a tal riguardo, il Collegio di coordinamento con decisione n. 22745/2019, pronunciandosi su quesiti interpretativi in tema di onere della prova del dolo o della colpa grave dell'utente, posto a carico del prestatore di servizi di pagamento, ha formulato il principio interpretativo secondo il quale: "la previsione di cui all'art. 10, comma 2, del d. lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente".

Da quanto sopra ne emerge che l'intermediario, dopo aver fornito prova della corretta autenticazione, registrazione e contabilizzazione dell'operazione, è chiamato ad indicare una serie di elementi di fatto circa la condotta della ricorrente dai quali possa trarsi prova della colpa grave della stessa.

Non trascura, il Collegio, l'apprezzamento sulla particolare insidiosità delle truffe perpetrate con la modalità dello spoofing (cfr. Coll Coord. 22745/19) ma d'altronde non si può però non tener conto del fatto che la ricorrente abbia agito con grave negligenza nel momento in cui ha omissso il controllo del conto corrente cui era associata la carta, per un notevole lasso di tempo.

Ciò detto, il Collegio rileva che il numero elevato di transazioni *online* (32) eseguite nell'arco di circa 20 giorni, peraltro eseguite per la maggior parte in orario notturno (tra le 22 e le 3 di mattina) verso uno stesso beneficiario e dunque effettuate con modalità sicuramente particolari rispetto all'operatività ordinaria del conto corrente della ricorrente, costituisca un macroscopico indice di anomalia che avrebbe dovuto insospettire e allertare i sistemi di monitoraggio dell'intermediario, inducendolo a porre in essere presidi di sicurezza idonei a salvaguardare il cliente dalle conseguenze di una frode palesatasi come estremamente probabile.

Alla luce di quanto sopra, il Collegio ritiene che si debba procedere ad una distribuzione in concreto di un concorso di colpa tra le parti e che, a tal riguardo, per la sua quantificazione, si possano valorizzare gli indici di anomalia previsti dal DM 112/2007 che sono espressione di un generale obbligo di monitoraggio delle operazioni da parte dell'intermediario.

Nel caso di specie, viene in rilievo l'indicatore di anomalia di cui alla lett. a), punto n. 2 (tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita): infatti, le operazioni non autorizzate a favore di un medesimo esercente sono 32, di cui, la seconda, la terza e la quarta effettuate a distanza di poco tempo una dall'altra (in particolare alle 00:25, 02:02, 02:04 e 02:08 del 21/07), per cui deve ritenersi che l'intermediario abbia colposamente omissso di attivarsi per impedire il rischio di frode normativamente tipizzato (*cfr.*, in termini, la decisione ABF, Collegio di Bologna, n. 11849/2017, nonché Collegio di Roma, n. 4131/2015 e n. 11452/2016).

Alla luce di quanto sopra, applicando l'indicatore sopra riportato, il Collegio ritiene di dover individuare un concorso di responsabilità tra le parti ed accerta il diritto della ricorrente al rimborso della somma di euro 3.904,00.

PER QUESTI MOTIVI

Il Collegio – in parziale accoglimento del ricorso – dichiara l’intermediario tenuto in favore della parte ricorrente alla restituzione dell’importo complessivo di euro 3.904,00 (tremilanovecentoquattro/00).

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

IL PRESIDENTE