

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) MARIANELLO	Membro designato dalla Banca d'Italia
(NA) SANDULLI	Membro di designazione rappresentativa degli intermediari
(NA) MAFFEO	Membro di designazione rappresentativa dei clienti

Relatore FEDERICA SANDULLI

Seduta del 25/11/2025

FATTO

La ricorrente, titolare di un conto corrente e di una carta di debito emessa dall'intermediario convenuto, riferisce che a seguito del furto in data 09.03.2025 del proprio cellulare (sul quale era installata l'*app* dell'intermediario) contattava i numeri di assistenza per bloccare la carta e il conto corrente collegato.

Gli operatori confermavano l'avvenuto blocco e l'impossibilità di sottrarre denaro. Il furto veniva altresì denunciato alle competenti autorità. Tuttavia, in data 10.03.2025, recandosi presso uno sportello dell'intermediario, apprendeva che il conto non era stato tempestivamente bloccato e risultavano ammanchi di denaro. Il blocco effettivo avveniva solo quella mattina dopo ulteriori solleciti. Compilava quindi il modulo di contestazione degli addebiti con i dati forniti dall'operatore.

L'Intermediario respingeva la richiesta di disconoscimento delle operazioni, sostenendo che le transazioni erano state correttamente autenticate. Al riguardo, la ricorrente contesta tale affermazione, evidenziando che si è trattato di furto con destrezza e che il sistema di autenticazione non avrebbe garantito adeguata sicurezza.

Chiede quindi di condannare l'Intermediario a riaccreditare l'importo sottratto in maniera fraudolenta, pari a euro 3.200,00. Chiede inoltre che l'intermediario depositi le registrazioni audio delle conversazioni telefoniche intercorse dalle utenze indicate nel periodo compreso tra il 09.03.2025 ore 16:50 e il 10.03.2025 ore 09:00, al fine di confermare la volontà di impedire qualsiasi addebito sul conto, nonché la lista dei movimenti con indicazione di luogo e orario delle operazioni contestate; il tutto oltre refusione delle spese legali.

L'intermediario, ritualmente costituitosi, precisa che le n. 12 operazioni contestate consistono in un

bonifico istantaneo, ricariche di carte e un prelievo *cardless*, tutti eseguiti tramite *app*, utilizzando le credenziali di sicurezza riconducibili alla ricorrente. Dalle verifiche effettuate emergerebbe che la ricorrente aveva registrato sul proprio dispositivo le credenziali di accesso. Il frodatore si sarebbe autenticato correttamente nell'*app* con tali credenziali nella data indicata e le transazioni risulterebbero eseguite e autorizzate secondo la normativa vigente, mediante procedura di autenticazione forte, ossia attraverso l'inserimento del codice di sicurezza “*ID” direttamente nell'*app*.

A parere dell'intermediario, ciò dimostrerebbe che la ricorrente conservava le credenziali di accesso insieme al dispositivo, circostanza che avrebbe reso possibile la truffa.

Inoltre, evidenza che il dispositivo oggetto di furto non era protetto da *password*, circostanza che avrebbe agevolato l'accesso ai dati sensibili e all'*app* da parte dei malfattori. Tale informazione sarebbe confermata anche dalle registrazioni delle chiamate al *call center*, in cui la ricorrente ribadisce che l'accesso al dispositivo era libero. Nella stessa chiamata, la cliente avrebbe riferito che erano già stati addebitati circa € 3.000,00 sul proprio conto.

Chiarisce che il blocco e l'estinzione della carta sono avvenuti alle ore 07:42 del 10.03.2025, quindi successivamente alle operazioni oggetto di controversia ed eccepisce l'infondatezza delle richieste risarcitorie avanzate dalla ricorrente per la refusione delle spese legali, considerato che il procedimento ABF è attivabile su istanza di parte e non richiede l'assistenza di un legale.

In sede di repliche, parte ricorrente ribadisce di aver immediatamente contattato, nel giorno della frode, il servizio clienti per bloccare la carta e il conto, ricevendo rassicurazioni sul blocco. Solo il giorno successivo, recatasi in filiale, avrebbe appreso che il conto non era stato bloccato tempestivamente e risultavano addebiti non autorizzati. Ribadisce altresì di non aver mai consentito le operazioni fraudolente, né di aver conservato il codice autorizzativo sul dispositivo.

Nelle proprie controrepliche, l'intermediario, riportandosi al contenuto delle controdeduzioni, insiste per il rigetto del ricorso.

DIRITTO

1. - La ricorrente, titolare di un conto corrente e di una carta di debito emessa dall'intermediario resistente, disconosce n. 12 operazioni per complessivi € 3.200,00 eseguite il 09.03.2025 tra le ore 19:18 e 20:41; dalle evidenze prodotte dall'intermediario emerge che le operazioni consistono in un prelievo *cardless* di € 600,00, in un bonifico istantaneo di € 600,00 ed in n. 10 ricariche di carte prepagate dell'importo di € 200,00 cadauna.

In particolare, la ricorrente riferisce che le operazioni disconosciute sarebbero state eseguite dal proprio *smartphone* tramite la *app* dell'intermediario da malfattori che lo avrebbero trafugato dalla tasca del suo cappotto mentre passeggiava in una via commerciale in data 09.03.2025 tra le ore 16:50 e le 17:00.

2. - Le operazioni disconosciute sono sottoposte alla disciplina dal d.lgs. n. 11/2010, modificato a seguito dell'entrata in vigore, in data 13.01.2018, del d.lgs. n. 218/2017, di recepimento della Direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno.

A fronte del disconoscimento delle operazioni di pagamento *on line* da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che le operazioni siano state autenticate, correttamente registrate e contabilizzate ai sensi degli artt. 10, commi 1 e 2 e 10-bis, comma 1 del d.lgs. 11/2010. In mancanza di tale dimostrazione, l'intermediario sopporta integralmente le conseguenze delle operazioni disconosciute. In particolare, è onere dell'intermediario provare di aver garantito al cliente un sistema di autenticazione forte, cioè “*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” (Art. 1, lett. q-bis, d.lgs. 11/2010). I prestatori di servizi di pagamento devono applicare l'autenticazione forte del cliente qualora l'utente: a) acceda al suo conto di pagamento *online*; b) disponga un'operazione di pagamento elettronico; c) effettui qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Il Regolamento Delegato (UE) 2018/389 individua come requisiti ai fini SCA due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza, purché indipendenti tra loro, nonché la presenza di un collegamento dinamico.

3. - L'intermediario resistente deduce di adottare due procedure di autenticazione forte: la procedura “primaria” con *Push notification* in *app* e Codice *ID e la procedura “secondaria” con *One Time Password* (OTP) via *sms* e *password*.

Con riferimento alla procedura primaria (utilizzata nel caso di specie) fornisce le note esplicative della stessa ove si legge che essa si basa sui seguenti elementi: a) Conoscenza: il codice *ID che è un codice di sei caratteri scelto dall'utente in fase di abilitazione dei prodotti finanziari in *app*; b) Possesso: la disponibilità del dispositivo dal quale precedentemente è stato generato il codice *ID.

Viene altresì dedotto dall'intermediario che anche l'attivazione del codice *ID avviene tramite una procedura di autenticazione forte che prevede: a) l'accesso all'*app* installata sul dispositivo dell'utente con credenziali personali (username e password); b) la abilitazione in *app* di almeno un prodotto finanziario utilizzando elementi di sicurezza specifici dei singoli prodotti; c) la scelta e la creazione di un codice alfanumerico.

L'intermediario, con riferimento alla fase di configurazione ed *enrollment* dello strumento di pagamento nella *app*, produce una schermata che attesta la registrazione della carta di pagamento della ricorrente al sistema autorizzativo di tipo dinamico, funzionante mediante invio con *sms* della *password* dinamica sul numero di cellulare indicato nella denuncia. Chiarisce, inoltre, che non vi è stato alcun cambio utenza dall'*enrollment* della carta fino alla chiusura.

Ha prodotto altresì l'estratto informatico dal quale si evince l'accesso in *app* nella data in cui sono state effettuate le operazioni contestate, il nome utente della ricorrente, il *device id* e la modalità identificativa (codice *ID).

Con riferimento alla fase dispositiva, l'intermediario deduce che le operazioni vengono disposte tramite l'inserimento del codice di sicurezza “*ID” al ricevimento della notifica in *app*.

Tale sistema è *compliant* (cfr. in tal senso Collegio di Roma, decisione n. 3507/2024) con gli *standard* dettati dalla normativa vigente e declinati dall'EBA, prevedendo più fattori riconducibili l'uno alla sfera della conoscenza esclusiva dell'utente (*ID), l'altro a quella del possesso (*app*).

In relazione alle singole operazioni contestate, l'intermediario produce le evidenze informatiche da cui si evince l'autorizzazione tramite il codice *ID ed il dispositivo della ricorrente (in uso ai malfattori a seguito del furto).

Con particolare riferimento al prelievo *cardless* di € 600,00 l'intermediario precisa che l'operazione - effettuata allo sportello - è stata autorizzata tramite *app* generante un QR CODE, con codice *ID. Dai log relativi al prelievo ATM, emerge l'utilizzo della *app* ma non del codice *ID. Tuttavia, anche per il prelievo *cardless* si può ritenere provata la SCA, come da ultimo in una situazione similare evidenziato dal Collegio di Roma: *“Per quanto ampiamente argomentato dalla resistente, tutte le transazioni sono avvenute all'interno di un sistema dinamico di autenticazione che prevedeva l'utilizzo del codice ***ID nell'App Banco***, che si sviluppa nel seguente modo: -previo accesso all'app andare alla sezione “Prelievo senza carta”; -recarsi presso un Atm e premere il pulsante dedicato; -inquadrare il codice QR mostrato sullo schermo dell'Atm; -inserire l'importo che si desidera prelevare, scegliendolo da un taglio predefinito o inserendolo manualmente, e confermare andando su “Procedi”; -inserire il codice P***I* e andare su “Conferma”.*

*Sulla base di tale descrizione, i fattori di autenticazione utilizzati risultano il codice P*id (fattore di conoscenza), e l'app dell'intermediario precedentemente associata a un dispositivo (fattore di*

possesso).

Secondo l'orientamento condiviso fra i Collegi, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati i log delle operazioni nonché gli ulteriori elementi esplicativi che consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione (Collegio di Roma, decisione n. 461/2025).

In conclusione, si ritiene che l'intermediario abbia dato prova dell'utilizzo di un sistema di autenticazione forte e della formale regolarità di tutte le operazioni contestate.

4. - Come chiarito dal Collegio di Coordinamento, con la decisione n. 22745/19: *“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”*.

Questo collegio ha evidenziato in argomento che l'intermediario deve *“provare la riconducibilità dell'operazione all'utente che la disconosca ovvero la frode o l'inadempimento doloso o gravemente colposo dell'utente stesso, nonostante l'apparentemente corretta autenticazione dell'operazione di pagamento”* e tale prova *“può ovviamente essere fornita pure per mezzo di presunzioni gravi, precise e concordanti, secondo quanto dispone l'art. 2729 c.c., di un comportamento fraudolento, doloso o gravemente colpevole dell'utente (ex multis cfr. Collegio Napoli, dec. 1091/2018). La stessa Corte di Cassazione, a tale specifico riguardo, ritiene che sia ammissibile la prova indiziaria della sussistenza della colpa grave (cfr. Cass. n. 654/2010)”* (Collegio di Napoli, decisione n. 19863/2021).

Nel caso di specie, l'intermediario resistente ritiene desumibile che il codice autorizzativo fosse colpevolmente conservato insieme al cellulare dal fatto che le operazioni contestate si siano verificate nel giorno stesso del furto del cellulare. Inoltre, ritiene verosimile che le credenziali e i codici fossero *“salvati nella memoria del telefono che si ribadisce non era protetto da password (come dichiarato dalla ricorrente nella conversazione con il call center)”*.

Non sono agli atti le registrazioni audio relative all'interlocuzione con il *call center* ed in sede di denuncia la cliente dichiara che il proprio *smartphone* era protetto da *“blocco schermo con codice di sicurezza”*.

Ebbene, secondo gli orientamenti condivisi dei Collegi, la condotta del ricorrente, che subisca lo smarrimento dello strumento di pagamento in un luogo pubblico è generalmente connotata da colpa grave, in quanto la soglia di attenzione dell'utilizzatore dovrebbe innalzarsi in relazione alla libera accessibilità al luogo pubblico da parte di terzi, fatta salva la valutazione di ulteriori circostanze del caso concreto. Nel caso di specie il telefono cellulare è stato sottratto dalla tasca del cappotto in una strada commerciale ed in un'ora in cui essa è notoriamente molto affollata e, come da ultimo chiarito dal Collegio di Bari, con decisione n. 8787/2025: *“Sulla configurabilità di un'ipotesi di furto con destrezza affermata dal ricorrente, la resistente sostiene che la sottrazione del portafoglio, con all'interno lo strumento di pagamento utilizzato, è avvenuta in un luogo pubblico (pubblica via) dove è pertanto richiesto alla clientela un grado di attenzione maggiore nella custodia dei propri effetti personali. Si deve rammentare che, condivisibilmente, i Collegi ritengono connotata da colpa grave la condotta del cliente che subisca il furto in un luogo affollato (come appunto accaduto nel caso di specie), in quanto la soglia di attenzione dell'utilizzatore dovrebbe innalzarsi in relazione alla libera accessibilità al luogo pubblico da parte di terzi (ex multis Collegio di Bari, decisione n. 4848/2025; Collegio di Roma, decisione n. 8573/24; Collegio di Milano, decisione n. 13381/24; Collegio di Palermo, decisione n. 11791/24)”*.

Vi è poi che i malfattori hanno potuto utilizzare l'*app* dell'intermediario ed effettuare subito dopo il furto le operazioni disconosciute perché hanno avuto libero accesso al contenuto del telefono cellulare rubato alla ricorrente che, pertanto, si può presumere non fosse protetto da codice di sblocco. Inoltre, la

ricorrente non ha provveduto a bloccare lo smartphone da remoto o cancellare tutti i dati presenti in esso sfruttando i sistemi antifurto inclusi “di serie” da Google e Apple nei propri *device*, così consentendo l'utilizzo dello stesso. Infine, attesa la necessità dell'utilizzo del codice personalizzato *ID sia per accedere alla *app* che per autorizzare le operazioni contestate, è presumibile che lo stesso fosse annotato nel dispositivo o conservato con esso.

In conclusione, il collegio ritiene che si configuri nella fattispecie la colpa grave di parte ricorrente.

5. – Inammissibile è la domanda tesa ad ottenere la condanna dell'intermediario a depositare le registrazioni audio della interlocuzione telefonica avvenuta tra la ricorrente e il numero verde dell'intermediario. In argomento è stato statuito: *“Come affermato dai Collegi territoriali, in particolare da Coll. Milano, dec. 7566/2023, “l’ascolto di un file audio sarebbe incompatibile con le modalità attraverso cui questo Arbitro procede in sede collegiale alla disamina del materiale probatorio offerto dalle parti e forma di conseguenza il proprio convincimento...[...] Sarebbe stato invece possibile acquisire come fonte di prova la trascrizione delle telefonate, ove fosse stata depositata dalla ricorrente. La prima domanda andrà dunque dichiarata inammissibile”* (Collegio di Bologna, decisione n. 7936/2025)

Infine, rispetto alla richiesta che l'Intermediario depositi la lista movimenti da cui si evincono luogo e orario delle operazioni, deve rilevarsi che dalle evidenze informatiche prodotte dall'intermediario si desume l'orario delle transazioni, non si evince anche il “luogo”, trattandosi di operazioni *online*, eseguite tramite *app* installata sul dispositivo della ricorrente.

6. – In conclusione, il ricorso non può trovare accoglimento avendo l'Intermediario provato sia che le operazioni disconosciute sono state correttamente autenticate, registrate e contabilizzate, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi, sia la colpa grave di parte ricorrente.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE