

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore FULVIO GIGLIOTTI

Seduta del 28/04/2026

FATTO

1. Con ricorso proposto in data 1.12.2025 – previo reclamo del 6.11.2025 – la ricorrente ha esposto che – dopo aver ricevuto sull'app dell'intermediario resistente due notifiche di pagamenti non autorizzati, bloccati dall'intermediario – veniva contattata da un sedicente operatore dell'intermediario, che la avvertiva della necessità di mettere in sicurezza il capitale sul conto, in ragione dell'avvenuta (asserita) duplicazione della carta in Romania.

Ha precisato, inoltre, che l'interlocutore conosceva dati riservati non dichiarati: saldo totale, presenza di franchi svizzeri e la sua residenza attuale (non aggiornata sull'app); con tono allarmato la sollecitava a convertire i franchi in euro; in simultanea riceveva SMS che si inserivano sulla precedente *chat* con intestazione dell'intermediario, riconducibili alla loro sezione antifrode, che confermavano la necessità di seguire le indicazioni telefoniche.

In questo contesto, la stessa, considerate l'urgenza e la minaccia di blocco della carta, autorizzava il trasferimento della somma di € 2.020,00, che (secondo le rassicurazioni ricevute) sarebbe stata subito riaccreditata.

Non ricevendo alcun rimborso, interrompeva la chiamata; il sedicente operatore antifrode tentava ancora di contattarla per farle trasferire il resto dei fondi (a lui noto), e in quel momento comprendeva la truffa della quale era rimasta vittima.

Ha quindi adito l'Arbitro, chiedendo – sul presupposto di una negligenza professionale del convenuto (che non avrebbe rilevato l'anomalia dell'operazione dispositiva e non avrebbe tenuto conto che le operazioni precedenti sul conto erano di importo modesto e di natura esclusivamente personale e non

speculativa) – la condanna dell’intermediario convenuto al rimborso della somma di euro 2.020,00, oltre interessi e spese.

2. Si è costituito l’intermediario, chiedendo il rigetto del ricorso.

In particolare, ha evidenziato parte resistente che si tratterebbe di operazione disposta personalmente dalla ricorrente, non disconoscibile.

In ogni caso l’operazione dispositiva risulterebbe anche regolarmente autorizzata, con rispetto della procedura di SCA richiesta.

Ha poi precisato che nessun obbligo di monitoraggio aveva esso resistente, e che, comunque, rispetto all’operazione posta in essere è stata inviata notifica *push*, descrittiva dell’operazione poi autorizzata.

Ha aggiunto, inoltre, che gli SMS ricevuti dalla cliente – seppur apparentemente provenienti dall’intermediario – presentano evidenti errori grammaticali e differenze stilistiche rispetto ai messaggi genuini; e che la ricorrente ha negligenzemente dato seguito alle richieste anomale del suo interlocutore, non assumendo rilevanza il fatto che le chiamate ricevute apparissero provenire dal numero verde del servizio clienti dell’intermediario in quanto il carattere anomalo delle richieste rivolte alla ricorrente avrebbe dovuto indurre quest’ultima a non seguire le indicazioni del falso operatore.

Ha quindi concluso per il rigetto del ricorso.

3. In sede di repliche, parte ricorrente ha insistito per l’accoglimento del ricorso.

DIRITTO

4. Ritiene il Collegio che la domanda della ricorrente sia parzialmente da accogliere, per le ragioni di seguito illustrate.

5. L’operazione contestata è stata posta 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), entrato in vigore il 13 gennaio 2018; le fonti normative che, nel contesto considerato, regolano la c.d. “autenticazione forte” (in gergo, individuata dall’acronimo SCA: *strong customer authentication*) sono rinvenibili negli artt. 97 e 98 della PSD2, nell’articolo 10-bis del D. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall’eba (*European Banking Authority*) e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall’EBA (in particolare, parere del 21 giugno 2019).

6. Secondo le previsioni normative sopra richiamate, riferibili alla fattispecie, la responsabilità di un Prestatore dei servizi di pagamento (PSP) è esclusa quando, *avendo esso dato prova di utilizzare meccanismi di “autenticazione forte” dell’utente*, sia anche riuscito a dimostrare una condotta dolosa o gravemente colposa dell’utente del servizio (con la precisazione che si intende per “autenticazione forte” 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).

Più in particolare, 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’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 D. lgs. n. 11/2010.

Piuttosto, sarà onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell’utente: in mancanza di ciò, egli sarà tenuto responsabile dei pregiudizi subiti dall’utente, in ragione del rischio d’impresa sopportato.

Ne consegue che l'intermediario non si libera dalla responsabilità provando la mera regolarità formale delle transazioni, dovendo lo stesso, ai sensi dell'art. 10 del D. lgs. n. 11/2010, documentare elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, anche in via presuntiva, della colpa grave (o del dolo) dell'utente (cfr. Collegio di Coordinamento ABF, n. 22745 del 10 ottobre 2019), fermo restando che in caso di mancanza di prova dell'avvenuto rispetto delle procedure di SCA richieste la responsabilità dell'intermediario andrà comunque dichiarata.

7. Peraltro, a diversa valutazione devono essere sottoposti i casi in cui il cliente, ancorché vittima di colpevole credulità, ponga in essere le operazioni contestate *direttamente e personalmente*, perché, in tal caso, la fattispecie...non è sussumibile nell'ambito del citato d. lgs. (in tal senso, *ex multis*: Coll. ABF Palermo, decisione n. 2090 del 4.2.2022; Coll. Palermo, decisione n. 10042 del 04.06.2020; Coll. Roma, decisione n. 4658/21 del 22.02.2021; Coll. Roma, 4962 del 23.3.2022).

Invero, in ragione della diretta riconducibilità al cliente dell'operazione posta in essere, vale allora la considerazione secondo la quale, per quanto la volontà del cliente di effettuare [l'operazione] possa essere viziata per effetto di raggiri di terzi, l'intermediario non può che considerare autorizzata l'operazione effettuata «personalmente dal titolare» (in tal senso, ad es., Coll. ABF Milano, n. 8602/2021).

In casi di tal genere, secondo unanime orientamento dei Collegi territoriali, non è certamente configurabile una responsabilità oggettiva del PSP; il Collegio potrà tuttavia rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, (solo) quando emerga, in concreto, dalla documentazione in atti, un *apporto causale* autonomo dell'intermediario, come, ad esempio, nei casi di:

- a) mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;
- b) mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore;
- c) mancato rilievo di indizi di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere.

Qualora, tuttavia, l'operazione sia stata solo parzialmente disposta dal cliente (ad es., in quanto l'operazione sia capziosamente "impostata" dal truffatore, e poi autorizzata, in quanto vittima dell'inganno, dal cliente), essa resta disconoscibile, e assoggettata alla disciplina del D. lgs. n. 11/2010 (salva la possibilità di valutare profili di concorso di colpa del cliente e dell'intermediario).

8. Alla luce del quadro normativo sopra richiamato, e della connotazione fattuale della vicenda per la quale si procede, per come risultante dalle evidenze in atti, rileva il Collegio che – differentemente da quanto predicato da parte resistente – non risultano evidenze, in atti, che si sia effettivamente trattato di operazione disposta interamente e personalmente dalla ricorrente (è verosimile, anzi, alla luce dei riferimenti forniti dalle parti, che l'operazione sia stata predisposta sul sito del *merchant* dal frodatore (in possesso dei dati della carta) e sia stata poi validata dalla ricorrente, mediante i due fattori di autenticazione).

Tanto premesso, rileva il Collegio che sono state prodotte evidenze attestanti il rispetto della procedura di SCA da parte dell'intermediario: l'operazione (come ammesso dalla ricorrente stessa) è stata autorizzata da device certificato nella disponibilità della ricorrente (elemento di possesso), mediante riconoscimento facciale (elemento di inerenza).

Risulta anche inviata una notifica *push* descrittiva dell'operazione autorizzata.

Come già anticipato, ciò non esclude possibili responsabilità, anche in concorso, da parte dell'intermediario.

9. La fattispecie per cui è sorta controversia integra, certamente, un caso di *spoofing*, che i Collegi territoriali valutano ordinariamente come frodi particolarmente insidiose, tali da poter anche escludere, solitamente, la colpa grave del cliente: peraltro, se nelle fattispecie di *spoofing* non è generalmente

ravvisabile la colpa grave del ricorrente, potrà essere però ravvisato un concorso di colpa tra le parti (in particolare, ad es., in presenza di indici di inattendibilità o anomalie del messaggio, anche in ragione della sua formulazione sintattica e grammaticale), in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di *phishing*; e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario.

10. Tenuto conto di quanto fin qui illustrato, rileva il Collegio che:

- la ricorrente ha dichiarato di avere eseguito le istruzioni impartite dall'ignoto interlocutore, in tal modo fornendo un apporto determinante alla consumazione della frode in suo danno;
- inoltre, i messaggi civetta ad essa inviati risultavano manifestamente privi di una veste professionale adeguata, con significative imperfezioni grammaticali e sintattiche;
- peraltro, l'aggressione a mezzo *spoofing* è stata preceduta – come confermano sia la ricorrente che il resistente – dal tentativo di eseguire due operazioni di pagamento di importo sotto la soglia per l'attivazione del protocollo 3DS, annullate o respinte. Le due transazioni sono servite come contesto per agevolare il successivo intervento del sedicente operatore dell'intermediario e accreditare l'idea che lo strumento di pagamento della ricorrente fosse stato violato;
- i dati dell'operazione, quali risultano dai *log* prodotti, parrebbero confermare che si tratti di un classico flusso *e-commerce*, invero poco coerente con la natura e i servizi offerti dall'intermediario genuino;
- l'intermediario resistente, da parte sua, non ha fornito alcun ragguaglio sulla reale identità del *merchant* e/o dell'*acquirer* attraverso il quale operava;
- appare verosimile che i fondi siano stati indirizzati verso un beneficiario fittizio, costituito al solo fine di realizzare il piano criminoso, utilizzando il *merchant descriptor* di un operatore bancario per assicurare la vittima e accreditare l'idea che si trattasse di un trasferimento per motivi di sicurezza;
- l'ipotizzata manipolazione non sarebbe stata intercettata né dall'*acquirer* che avrebbe introdotto il sedicente *merchant* nel circuito, né dall'odierno resistente, il quale non avrebbe rilevato l'incoerenza tra operazione, identità effettiva del beneficiario e *merchant descriptor*.

11. Alla luce delle risultanze emerse, reputa il Collegio che debba essere senz'altro predicata l'esistenza di un concorso di colpa delle parti, seppure con maggior apporto contributivo da parte della ricorrente: concorso che può essere ragionevolmente stimato nella misura di un terzo a carico dell'intermediario resistente e di due terzi a carico della ricorrente.

Ne consegue che parte resistente sarà tenuta a rimborsare alla ricorrente, in ragione del concorso di colpa predicabile, la somma di euro 674,00, oltre interessi dal reclamo

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente al risarcimento del danno nella misura equitativamente determinata di € 674,00, oltre interessi legali dalla data del reclamo.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE