

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) VERDICCHIO	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO VERDICCHIO

Seduta del 11/12/2025

FATTO

La ricorrente riferisce di aver ricevuto, in data 12/03/2025, un *sms* apparentemente proveniente dall'intermediario convenuto, con cui veniva allertata circa alcune operazioni non autorizzate; alla ricezione del messaggio, contattava il numero indicato. Rassicurata dal fatto che questo risultava riconducibile all'intermediario, ella confermava i propri dati personali e subiva due addebiti non autorizzati, rispettivamente di euro 10.000,00 e di euro 2.000,00, riconducibili, il primo, a un'operazione di bonifico e, il secondo, a un pagamento *online* tramite carta di debito.

Resasi conto di essere rimasta vittima di truffa, contattato l'intermediario, bloccava il conto e provvedeva altresì a sporgere denuncia.

La ricorrente lamenta, al riguardo, che la banca non impediva le operazioni in contestazione, benché – a suo dire – di natura anomala, e non adottava adeguate misure antifrode. Insoddisfatta dell'interlocuzione prodromica al ricorso avuta, ritenendo che, in assenza – a suo dire – di autenticazione forte, la responsabilità non possa ricadere sul cliente, la stessa si rivolge all'Arbitro chiedendo il rimborso della somma di euro 12.000,00, maggiorata delle spese di assistenza difensiva. Soltanto nelle repliche la ricorrente chiede, altresì, la rivalutazione monetaria e gli interessi legali sulla somma principale richiesta.

L'intermediario, ritualmente costituitosi, rappresenta che la richiesta di rimborso risulta infondata, in quanto le due operazioni disconosciute sono state correttamente autorizzate con autenticazione a due fattori, in assenza di malfunzionamenti.

Descrive, quindi, nel dettaglio i passaggi operativi e autorizzativi necessari per eseguire le due

operazioni contestate, facendo constare come essi siano pienamente conformi alle regole in tema di SCA. Sul punto la resistente richiama a sostegno numerose decisioni arbitrali secondo cui il sistema SCA predisposto risulta *compliant*.

Chiarito, dunque, che essa adotta un sistema di autenticazione forte per l'accesso all'area riservata, le disposizioni di bonifico e le operazioni di pagamento *online*, la resistente evidenzia che tutti i passaggi citati risultano essere stati correttamente realizzati per le operazioni in oggetto, fornendone evidenza. La resistente, nello specifico, sottolinea che in data 12/03/2025:

- alle ore 12:41:24 e alle ore 12:54:01, sono stati registrati due accessi con riconoscimento biometrico, precedentemente attivato, dall'abituale dispositivo in uso alla ricorrente;
- l'ultimo accesso con autenticazione forte del cliente era stato eseguito in data 27/01/2025 con codice OTP ricevuto tramite *sms* sul numero certificato;
- all'interno della seconda sessione di accesso, alle ore 13:00:22, è stato disposto ed eseguito personalmente e autonomamente dalla ricorrente il bonifico di euro 10.000,00 con autenticazione forte, ovvero accesso all'area riservata con riconoscimento biometrico (primo fattore) e utilizzo di conferma con *token* (secondo fattore);
- in seguito, alle ore 13:03:09, è stato registrato un ulteriore accesso dall'abituale dispositivo con riconoscimento biometrico;
- alle ore 13:07:33 è stata registrata la consultazione del PIN della carta di debito tramite conferma con *token*;
- successivamente, alle ore 13:08:22 e alle ore 13:09:54, sono stati registrati due accessi da *web* mediante inserimento di *username* e *password*, nonché OTP ricevuto tramite *sms* sul numero certificato;
- di conseguenza, alle ore 13:10:25, è stata registrata una modifica della *password* correttamente completata grazie ad accesso con *username* e *password* e inserimento di due cifre del PIN randomicamente scelte dal sistema. Il PIN della carta era stato visualizzato poco prima dalla ricorrente e, pertanto, inserito o comunicato;
- alle ore 13:12:35 è stata registrata la generazione di un CVV dinamico della carta con doppio fattore (ovvero accesso con *username* e *password* e inserimento di codice OTP, ricevuto tramite *sms*);
- alle ore 13:13:45 è stato eseguito il pagamento di euro 2.000,00 con autenticazione forte: inserimento dei dati statici della carta - PAN e data di scadenza - nonché del CVV dinamico generato (fattore di conoscenza) e inserimento di OTP ricevuta con messaggio *sms* (fattore di possesso) sul cellulare.

Ciò posto, la resistente ritiene di aver dimostrato che le operazioni in contestazione sono state eseguite dalla stessa ricorrente, nonché correttamente autorizzate mediante autenticazione forte e che, dalla ricostruzione esposta in denuncia, può ragionevolmente dedursi come nel caso in esame siano rinvenibili, in capo alla ricorrente, elementi di colpa grave (in violazione degli artt. 7 del d.lgs. 11/2010 e 43 dell'Accordo Quadro).

Quest'ultima, invero, contattava personalmente il sedicente operatore e disponeva personalmente il bonifico, cui, pertanto, non sarebbe applicabile la disciplina speciale delle operazioni non autorizzate. Inoltre, forniva altresì le OTP per eseguire le operazioni descritte e autorizzare il pagamento *on line*, nonostante il testo di accompagnamento delle conferme dei pagamenti fosse "parlante" e molto chiaro. Sul punto la resistente aggiunge che, anche qualora si provasse che la cliente è stata indotta da terzi a eseguire il riferito bonifico, la banca non poteva che considerare tali operazioni autorizzate, non potendo essere a conoscenza di ciò che accade al di fuori dell'area riservata.

La resistente evidenzia inoltre nelle controrepliche, in merito alla tempestiva segnalazione, che l'ordine di bonifico oggetto di contestazione è stato inserito con data di pagamento in pari giornata e che, quando la cliente ha informato il Servizio clienti, l'operazione risultava già eseguita e non più revocabile. Come previsto dal contratto, l'ordine è ricevuto dalla banca nel momento in cui il bonifico viene autorizzato mediante procedura a doppio fattore e "*il cliente non può revocare un ordine di pagamento dopo che è stato ricevuto dalla Banca*" (cfr. art. 37 del contratto e 17 del d.lgs. 11/2010).

Similmente, non possono essere revocati dopo essere stati ricevuti dal prestatore di servizi di pagamento, i pagamenti con carta di debito, essendo questa una “*tessera di pagamento o di prelievo con addebito immediato sul proprio conto*”.

In conclusione, ritenendo – anche alla luce della giurisprudenza arbitrale richiamata – di aver dimostrato che i fatti per cui si controverte sono ascrivibili al negligente comportamento della controparte, la banca chiede il rigetto del ricorso.

DIRITTO

La ricorrente, nel riferire di aver ricevuto un messaggio apparentemente proveniente dall'intermediario, ammette di aver contattato il numero di telefono in questione e di aver fornito dati riservati. La resistente asserisce, quindi, che le credenziali di sicurezza sono state fornite al truffatore direttamente dalla ricorrente e, in ogni caso, che il bonifico in questione è stato disposto personalmente e interamente dalla cliente con conseguente inapplicabilità allo stesso dello speciale regime di *favor* probatorio disposto dalla disciplina in tema di SCA. Trattasi, come noto, della disciplina recata dal d.lgs. n. 11/2010, modificato a seguito dell'entrata in vigore, in data 13/1/2018, del d.lgs. n. 218/2017, di recepimento della Direttiva (UE) 2015/2366 (c.d. PSD2), relativa ai servizi di pagamento nel mercato interno.

In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10-*bis* del d.lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14/9/2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21/6/2019). Va tenuto presente, inoltre, anche l'art. 12 del d.lgs. 11/2010, circa il rispetto, da parte dell'utente, degli obblighi di cui all'art. 7.

Ciò posto, dalla documentazione in atti risulta che, alle ore 12:41:24 e alle 12:54:01 del 12/3/2025, sono stati registrati due accessi tramite riconoscimento biometrico, precedentemente attivato dall'abituale dispositivo in uso alla ricorrente, e che tale dispositivo risultava già in uso alla ricorrente nei giorni precedenti.

Si precisa che la banca, nelle controdeduzioni, riferisce di avvalersi dell'art. 10 del Regolamento Delegato (UE) n. 389/2018/, come modificato dal Regolamento Delegato (UE) n. 2360/2022, che autorizza i PSP a non applicare l'autenticazione forte del cliente qualora non siano trascorsi 180 giorni dall'ultima volta che il cliente ha avuto accesso al conto (cfr. sul punto, *ex multis*, Collegio di Torino, decisione n. 9705 del 2024) mediante autenticazione forte, e documenta che l'ultimo accesso con autenticazione forte del cliente era stato eseguito in data 27/01/2025 con codice OTP ricevuto tramite *sms* sul numero di cellulare certificato, coincidente con quello indicato in denuncia.

Ad ogni modo, nel caso in esame, i due accessi nella giornata della frode sembrano avvenuti con doppio fattore (1. elemento di inerenza: riconoscimento biometrico; 2. elemento di possesso: app su device certificato della ricorrente).

Con riferimento al bonifico di euro 10.000,00, si rileva che esso è stato inserito alle ore 13:00:22 e autorizzato con autenticazione forte, cioè riconoscimento biometrico e conferma con *token* (secondo fattore). L'operazione è stata posta in essere dall'abituale dispositivo, sicché l'intermediario ritiene che essa sia stata eseguita personalmente dalla ricorrente. E tale valutazione appare quantomeno verosimile.

Alle ore 13:03:09 è stato registrato un ulteriore accesso dall'abituale dispositivo con riconoscimento biometrico. Alle ore 13:07:33 è stata registrata la consultazione del PIN della carta. L'operazione sembra essere stata autorizzata con doppio fattore di inerenza e di possesso.

Successivamente, alle ore 13:08:22 e 13:09:54 sono stati registrati due accessi da web con autenticazione forte, mediante inserimento di *username* e *password*, nonché OTP ricevuto tramite *sms*

sul numero di cellulare certificato.

Al riguardo si osserva che, nelle repliche, la ricorrente evidenzia che le operazioni provenivano da dispositivi diversi dal proprio; l'intermediario precisa che si tratta di accessi avvenuti da web, e dalle evidenze in atti pare comunque potersi escludere che sia stato certificato un nuovo *device* (attività che avrebbe richiesto una procedura di *enrollment* presidiata da SCA).

Alle ore 13:10:25 è stata registrata una modifica della *password*, a seguito di accesso effettuato con *username* e *password* più OTP, nonché inserimento di due cifre del PIN (che era stato visualizzato poco prima) randomicamente scelte dal sistema.

Alle ore 13:12:35 è stata registrata la generazione di un CVV dinamico della carta con doppio fattore: accesso con *username* e *password*; inserimento di codice OTP ricevuto tramite *sms* sul numero di cellulare certificato.

Alle ore 13:13:45 veniva eseguito il pagamento di euro 2.000,00 con autenticazione forte: inserimento dei dati statici della carta (PAN e data di scadenza), nonché del CVV dinamico appena generato (fattore di conoscenza); inserimento di OTP ricevuta con messaggio *sms* "parlante" (fattore di possesso) sul numero di cellulare certificato.

Con riferimento al procedimento di generazione del cd. CVV dinamico, esso, con riferimento a fattispecie simile a quella qui in contestazione, è stato giudicato conforme alla normativa SCA: cfr. Collegio di Napoli, decisione n. 11679 del 2024; Collegio di Roma, decisione n. 8749 del 2024.

I dati sopra evidenziati (sia nella parte in fatto che in quella in diritto) rendono fortemente verosimile che quantomeno il bonifico sia stato disposto personalmente dalla ricorrente; in ogni caso, per esso, sono state pienamente rispettate le disposizioni in tema di SCA.

Anche la seconda operazione contestata, pur essendo avvenuta via web, è verosimilmente stata effettuata dal consueto *device* in uso alla ricorrente, quindi personalmente, dal momento che sembra potersi escludere la certificazione di un nuovo *device*; in ogni caso, pure per essa risultano pienamente rispettate le disposizioni in tema di SCA.

A fronte di tali rilievi, non emergono elementi di anomalia, posto che entrambe le operazioni contestate erano contenute entro i limiti massimi di spesa consentiti.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE