Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) BULLO	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 STEFANO TRAVERSI

Seduta del 23/09/2025

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

FATTO

Con ricorso presentato in data 13/5/2025 la ricorrente deduce quanto segue:

- è titolare di una carta associata ad un conto corrente aperto presso l'odierno convenuto;
- in data 27/04/2025 riceveva, in una chat all'interno della piattaforma di vendita online S*.it, un documento PDF contenente un link ad un sito web fraudolento, apparentemente riconducibile all'intermediario convenuto, nel quale inseriva le proprie credenziali;
- il documento PDF sembrava provenire dal servizio di supporto ufficiale della piattaforma S*.it e riguardava una reale compravendita da lei effettuata;
- le venivano quindi addebitati due pagamenti da € 499,00 cad. (totale € 998,00), da lei non riconosciuti, verso il beneficiario R*R*, servizio interno alla banca convenuta.
- Parte resistente, nel controdedurre, afferma ed eccepisce che:
- le operazioni contestate erano autorizzate mediante procedura di autenticazione forte 3DS, in particolare per mezzo della ricezione di una notifica push sul dispositivo associato all'account della ricorrente e di riconoscimento biometrico digitale;
- la ricostruzione della truffa, operata dalla ricorrente, è incompleta, dal momento che mancano evidenze del PDF contenente il link fraudolento e della schermata del sito contraffatto;
- le due operazioni di pagamento disconosciute, eseguite a distanza di circa venti minuti l'una dall'altra, risultano intervallate da un'operazione di ricarica pari a € 499,00, somma poi integralmente utilizzata nella seconda transazione, ciò che fa presumere che la ricorrente abbia seguito specifiche istruzioni dettate da terzi;
- in seguito a ciascuna operazione disconosciuta, inviava sul dispositivo della ricorrente una notifica riportante l'ammontare speso;
- verosimilmente, la ricorrente, dopo avere cliccato sul link di phishing, inseriva i dati della propria carta sul sito truffaldino, permettendo così a terzi di inizializzare il pagamento a favore del beneficiario R*R*;
- in seguito, la stessa ricorrente autorizzava e finalizzava le operazioni, atteso che il riconoscimento biometrico digitale è a lei incontrovertibilmente riconducibile;
- pertanto, le operazioni di pagamento devono correttamente considerarsi quali operazioni effettuate personalmente dalla cliente, seppur sulla base di un consenso viziato, con conseguente inapplicabilità del D.Lgs. n. 11/2010;
- R*R*, beneficiario delle operazioni contestate, è un servizio interno al gruppo di cui è parte, che permette di acquistare criptovaluta con una carta o con il saldo del conto e di inviarla a un portafoglio di criptovaluta esterno a scelta dell'acquirente;
- nel caso di specie, quindi, il terzo frodatore, titolare di un account R*R*, dopo essersi impossessato dei dati della carta, induceva la ricorrente ad eseguire dei pagamenti per l'acquisto di criptovalute;

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

- le criptovalute così acquistate erano automaticamente trasferite su un wallet esterno di cui non ha la visibilità e sul quale non può operare per recuperare le somme;
- non è legittimata a fornire i dati del titolare dell'account R*R* coinvolto nel caso di specie, poiché tale account è gestito da un altro soggetto del gruppo bancario;
- il phishing deve oggigiorno considerarsi un fenomeno noto, anche per l'attenzione data dai mezzi di comunicazione di massa;
- anche la piattaforma di acquisti S* mette a disposizione degli utenti una pagina sul proprio sito, dedicata alla descrizione del phishing e dei comportamenti da seguire per evitare di esserne vittima;
- la condotta della ricorrente era connotata da colpa grave: cliccava link sospetti ed inseriva i propri dati personali e, presumibilmente, anche i dati della propria carta su pagine sospette; dava seguito alle richieste di pagamento ricevute; ricaricava il proprio conto dopo la prima operazione.

DIRITTO

Nella presente vicenda parte ricorrente richiede il rimborso di due operazioni non autorizzate effettuate con carta emessa dall'intermediario in data 27/04/2025 per un importo complessivo di € 998,00;

L'intermediario chiede il rigetto del ricorso perché infondato in fatto e in diritto e non provato.

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.

Occorre preliminarmente valutare l'applicabilità, al caso di specie, della disciplina prevista dal D.lgs. n. 11/2010 in caso di operazioni non autorizzate.

Secondo l'orientamento condiviso dai Collegi l'operazione eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD.

In questi casi, non è configurabile una responsabilità oggettiva del PSP, ma si potrà comunque rilevare un'eventuale responsabilità concorrente sulla base delle evidenze disponibili e secondo le norme di diritto comune, ove si ravvisi un contributo causale alla realizzazione della frode. Tali principi sono stati ribaditi dal Collegio di Coordinamento nella recente decisione n. 8671/2024.

La ricorrente sostiene nel ricorso di non avere autorizzato le operazioni di pagamento, affermando di aver cliccato un link contenuto in un PDF, inviatole sulla chat della piattaforma di vendita tra privati S*.it; il link la rimandava ad un sito web clone apparentemente riconducibile all'intermediario convenuto. Nella chat del 03/05/2025, la ricorrente riferiva di avere fornito le proprie credenziali all'interno del sito

fraudolento (cfr. all. 5 al ricorso). Nella denuncia allegata al ricorso, la ricorrente riferisce di non avere disposto tali transazioni.

L'intermediario eccepisce l'inapplicabilità della normativa di cui al. D.lgs. n. 11/2010 in materia di operazioni non autorizzate, dal momento che le operazioni in contestazione sono state autorizzate dalla ricorrente stessa, seppur in presenza di un consenso viziato.

In particolare, sostiene che la ricorrente ha autorizzato le operazioni di pagamento inizializzate dal truffatore dopo aver cliccato sul link di phishing, inserendo i dati della propria carta sul sito truffaldino, consentendo a terzi di inizializzare il pagamento fraudolento, disposto con riconoscimento biometrico digitale incontrovertibilmente riconducibile all'utente e al dispositivo. Deduce pertanto si verta in caso di operazione autorizzata dalla parte.

Le evidenze in atti inducono a ritenere fondate le eccezioni dell'intermediario circa il fatto che le operazioni contestate siano state eseguite con il consenso della ricorrente, in conformità con quanto previsto dai Termini dalle Condizioni Personali di Contratto (stralcio controdeduzioni). Si rileva altresì che le due operazioni di pagamento risultano intervallate da un'operazione di ricarica pari a € 499,00, somma poi integralmente utilizzata nella seconda transazione, circostanza che fa presumere che la ricorrente, nell'ambito della truffa che l'ha vista coinvolta, abbia seguito specifiche istruzioni dettate da terzi e le abbia disposte direttamente, nulla affermando o contestando riguardo questo accredito.

In ordine poi all'autenticazione delle operazioni, esse risultano disposte con il doppio fattore SCA con elemento di possesso (notifica push inviata sul device della ricorrente inviata sull'app che l'utente aveva a suo tempo installato sul proprio dispositivo) ed elemento di inerenza (riconoscimento biometrico digitale, fingerprint). Si rileva che il Collegio di Bologna ha ritenuto provata la SCA in presenza di fattori di autenticazione analoghi a quelli del caso di specie, decidendo un ricorso presentato nei confronti del medesimo intermediario odierno convenuto (Coll. Bologna, decisione n. 5775/25 – non ancora pubblicata).

In ordine alla dinamica dei fatti ed alla valutazione del comportamento tenuto dall'esponente, la frode è inquadrabile nello schema del c.d. phishing: la ricorrente ha infatti cliccato su un link sospetto, riportato su un documento PDF inviatole da un falso operatore del servizio di supporto della piattaforma S*.it, nell'ambito di una compravendita alla quale lei aveva partecipato. Cliccando il link, veniva reindirizzata ad una falsa pagina web dell'intermediario e qui inseriva le proprie credenziali.

Si configura pertanto una colpa grave della ricorrente – per avere inserito propri dati in link sospetti, dovendosi altresì rilevare che la ricostruzione dei fatti e la documentazione prodotta dalla Cliente risultano incomplete. In particolare, la stessa non ha fornito né evidenza dell'interfaccia del sito asseritamente imitato, né il file PDF contenente il link di phishing.

Parte ricorrente non ha allegato copia o screen-shot del PDF contenente il link truffaldino, non ha prodotto screen-shot del falso sito dell'intermediario, né ha allegato alcuna schermata della piattaforma S*.it.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Secondo l'orientamento condiviso dei Collegi, la mancata allegazione, da parte del cliente, di evidenze dell'avvenuto "accalappiamento" tipico del phishing (quali e-mail/sms civetta contenenti link truffaldini), determina il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e sia pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio (cfr. ex multis Collegio di Bologna, decisione n. 11920 del 26.8.2022).

Per tale insieme di motivi, il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
CHIARA TENELLA SILLANI