

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) CORRADI	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO VELLA

Seduta del 31/03/2026

FATTO

Il ricorrente, premesso di essere titolare di carta di credito n. ***9447 emessa dall'intermediario convenuto, come di seguito ricostruisce i fatti accaduti. In data 16/12/2024 riceveva un SMS sulla propria utenza telefonica, proveniente da un numero di telefonia mobile sconosciuto, contenente l'avviso della necessità di aggiornare i dati per poter ricevere la consegna di un pacco. Essendo effettivamente in attesa di ricevere una spedizione, cliccava sul link ivi contenuto ed inseriva i dati richiesti nella schermata richiamata: in particolare i dati anagrafici e quelli della carta di credito. Procedeva poi ad autorizzare il pagamento apparentemente di Euro 0,00, ricevendo tuttavia – subito dopo – l'avviso di una transazione effettuata per Euro 890,30. Si rendeva conto poi di essere incorso in errore, ritenendo che il numero prospettato nella schermata autorizzativa fosse l'identificativo della spedizione, mentre corrispondeva all'importo del pagamento da autorizzare espresso in valuta straniera (Rupie Indonesiane). Scoperta la truffa, si recava immediatamente presso la filiale di competenza per segnalare l'accaduto, bloccare la carta e domandare il blocco del pagamento, che tuttavia veniva comunque addebitato. Dopo aver sporto denuncia, trasmetteva il formale disconoscimento e poi successivo reclamo, entrambi riscontrati negativamente dall'intermediario convenuto. Ritenendo sussistente la responsabilità dell'istituto emittente lo strumento di pagamento in ragione del mancato blocco di operazione palesemente anomala, peraltro eseguita a seguito di un

errore dovuto alla opacità delle informazioni nella schermata autorizzativa del pagamento – che appariva di importo pari a zero –, parte ricorrente si determinava alla proposizione delle proprie istanze restitutorie dinanzi all'Arbitro, chiedendo il rimborso dell'operazione fraudolenta.

In via preliminare l'intermediario resistente domanda la declaratoria di inammissibilità del ricorso per l'inapplicabilità della disciplina di maggior tutela relativa alle transazioni non autorizzate, in quanto il ricorrente ha ammesso di aver autorizzato direttamente la transazione contestata, seppure con volontà sviata dall'errore in cui è incorso. Osserva sul punto che le affermazioni confessorie della controparte sono peraltro confermate dalla circostanza che il pagamento in questione risulti correttamente autenticato mediante doppio fattore SCA, rappresentato dalla notifica in App sul device del ricorrente e autorizzazione con riconoscimento biometrico.

Nel merito, afferma l'assenza di ogni sua responsabilità in quanto l'operazione contestata risulta correttamente registrata e contabilizzata, autorizzata con procedura conforme alle prescrizioni normative sul punto, mediante il device in uso del ricorrente e dal medesimo collegato all'App di gestione dello strumento di pagamento tre anni prima il fatto contestato. Al contrario, apparirebbe evidente la colpa grave del ricorrente, insita nell'aver confidato sulla genuinità di un messaggio proveniente da un mittente sconosciuto, contenente errori ortografici e che rinviava ad un link parimenti oscuro. Il medesimo quindi, con ingenua credulità, ha inserito i dati della propria carta di credito ed autorizzato un presunto pagamento di Euro 0,00 nella convinzione di dover sbloccare la ricezione di una consegna da parte di uno spedizioniere, evidentemente ignorando il testo "parlante" della notifica push ricevuta nella fase autorizzativa. Inoltre nega la sussistenza di un obbligo di monitoraggio delle transazioni in ipotesi anomale e non usuali ad eccezione delle casistiche indicate nel DM 112/2007. Evidenzia altresì come la Polizia postale sul proprio sito avesse pubblicato da tempo l'alert riferito alle truffe analoghe a quelle in cui è incorso il ricorrente e lo stesso intermediario resistente avesse implementato campagne informative per prevenire comportamenti quali quelli tenuti dalla parte attrice, tra cui quello di selezionare link contenuti in messaggi provenienti da mittenti sconosciuti. Precisa, infine, come ai sensi del D. Lgs. 11/2010 la transazione, una volta autorizzata, fosse irrevocabile.

Chiede il rigetto del ricorso.

DIRITTO

In via preliminare il Collegio rileva che le due eccezioni preliminari della resistente - che domanda la reiezione (ovvero la inammissibilità, nella parte iniziale delle controdeduzioni) del ricorso in quanto la transazione è stata autorizzata dal titolare stesso nonché per la mancanza di allegazioni in ordine alla truffa asseritamente subita -, attenendo al merito della controversia, saranno esaminate unitamente alle altre questioni di merito.

Il Collegio precisa che 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), 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.

Tanto precisato, con il ricorso il ricorrente contesta una transazione di pagamento online effettuata in data 16/12/2024 con la propria carta di credito n. ***9447 per l'importo di Euro 874,99 (oltre Euro 15,31 per commissioni di cambio) domandando quindi la rifusione di complessivi Euro 890,30.

Secondo l'orientamento dell'ABF, affinché un'operazione possa dirsi non autorizzata e, dunque, trovare applicazione la disciplina di diritto speciale che individua le responsabilità nel caso di operazioni non autorizzate, di particolare favor nei confronti dell'utente, approntata dal D. Lgs. n. 11/2010, deve difettare il requisito del "consenso del pagatore" di cui all'art. 5 del medesimo decreto, ipotesi che non si può ritenere sussistere nel caso in cui l'operazione sia personalmente, interamente ed autonomamente eseguita dal titolare dello strumento, come emerge nel caso in esame. In base alla documentazione in atti ed alle dichiarazioni rese sia nel ricorso che in denuncia, infatti, il pagamento contestato risulta correttamente autorizzato con il device in uso al medesimo ricorrente, senza che emergano risultanze di enrollment su altri dispositivi, e lo stesso dichiara di averlo personalmente eseguito, ammettendo di aver autorizzato il pagamento confondendo l'importo della transazione con il numero di spedizione. L'utente, in tali casi, resta pertanto pienamente responsabile per l'operazione eseguita.

Peraltro, date queste circostanze, secondo il medesimo orientamento condiviso, ove l'operazione sia eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), potrebbe venire in rilievo una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode. Si tratta di circostanza che, non presenti o non supportate da alcuna prova, non possono ritenersi rinvenibili nel caso in esame. Inoltre, come eccepito dalla resistente, il messaggio civetta è stato inviato da un numero di cellulare sconosciuto, non riconducibile a corrieri/spedizionieri e non in cronologia con altri eventuali precedenti messaggi genuini ed il link a cui il medesimo rinviava era parimenti ignoto e non identificabile come attendibile rispetto al suo contenuto ed al sedicente mittente. Ancora, come già sottolineato, il ricorrente ha ammesso di aver autorizzato il pagamento confondendo l'importo della transazione con il numero di spedizione, errore che non è stato sventato nemmeno dal testo del messaggio parlante inviato in fase autorizzativa sulla app del ricorrente, con il quale era notificata una specifica e dettagliata indicazione della transazione che si stava autorizzando. In ultimo, l'SMS truffaldino conteneva errori ortografici che avrebbero dovuto allertare sin da subito il ricorrente. Si tratta di circostanze ed elementi che avrebbero dovuto indurre la parte ricorrente ad un comportamento più attento e prudente e egli è pertanto chiamato a sopportare l'itera perdita subita.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE