

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) CARATOZZOLO	Membro designato dalla Banca d'Italia
(TO) ISAIA	Membro di designazione rappresentativa degli intermediari
(TO) PUDDU	Membro di designazione rappresentativa dei clienti

Relatore ISAIA

Seduta del 30/09/2025

FATTO

Parte ricorrente ha affermato di esser rimasta vittima di una truffa realizzata tramite sms, apparentemente inviate dall'intermediario resistente con il quale veniva informata dell'associazione di un dispositivo e invitata a contattare il numero ivi indicato per il disconoscimento di tale operazione. Chiamando l'utenza mobile, come da indicazioni, si è interfacciata con un sedicente operatore di parte resistente, il quale le comunicava che per ragioni di sicurezza avrebbe dovuto dissociare il suo *device* e riassociarlo in un secondo momento. Richiamata da un altro apparente funzionario di parte resistente, come anticipato dal malfattore in occasione della precedente telefonata, verificava che il numero da cui la stava chiamando corrispondeva al numero "*blocco carta*" dell'intermediario resistente, fugando i dubbi sull'identità dell'interlocutore. Confortata da questa corrispondenza, parte ricorrente ha quindi effettuato l'accesso in app, seguito le istruzioni fornite dal truffatore e dissociato il suo *device*. Il sedicente operatore provvedeva così ad associare il suo dispositivo ed effettuava un pagamento di € 3.485,00 su un sito di scommesse sportive. Parte ricorrente ha rappresentato di ritenere ingiustificabile il fatto che malviventi si siano inseriti nei server dell'intermediario e abbiano utilizzato i numeri di quest'ultimo per realizzare frodi a danno dei clienti. Inoltre, non era stata informata dall'intermediario resistente della presenza di un "*bollino di sicurezza in app*" a garanzia dell'autenticità degli operatori telefonici e a protezione degli utenti dalle truffe. Parte ricorrente domanda pertanto il rimborso della somma di € 3.485,00, pari al valore dell'operazione di pagamento disconosciuta.

Nelle controdeduzioni, l'intermediario resistente ha, *in primis*, rappresentato che la transazione è stata eseguita tramite Strong Customer Authentication (SCA), conformemente al D.Lgs. n. 11/2010, e resa nota alla parte ricorrente attraverso l'invio di una notifica *push* e un sms di esecuzione del pagamento oggetto di contestazione. La truffa, eseguita secondo uno schema frodatorio ormai noto, è scaturita dal messaggio truffaldino ricevuto dalla ricorrente, la quale effettuava e riceveva chiamate da utenze non riferibili alla resistente, che afferma di relazionarsi con la propria clientela secondo altre modalità. Parte ricorrente è quindi caduta vittima di colpevole credulità, avendo rilasciato ai vari interlocutori telefonici i dati richiesti, ovvero tutti i codici OTP ricevuti. Le stesse condizioni contrattuali sottoscritte (aggiornate alla proposta di modifica unilaterale comunicata in data 23/04/2024) esplicitano che, in caso di ricezione di una e-mail o telefonata sospetta che simula una comunicazione dell'intermediario, il cliente è tenuto a non darvi seguito e a contattare il servizio di assistenza clienti. L'intermediario ha, quindi, affermato che parte ricorrente versa in colpa grave, considerando anche che aveva a disposizione il c.d. *"bollino di sicurezza"* in *homebanking*, come comunicatole con mail del 05/07/2024 e indicato sul sito internet della banca. Oltre a questo presidio di sicurezza, parte ricorrente aveva ricevuto e-mail e notifiche *push* specifiche delle varie campagne di sensibilizzazione svolte dall'intermediario finalizzate alla prevenzione di truffe informatiche quale quella in esame. Infine, parte resistente ha richiamato che il contratto in essere con la ricorrente enuncia espressamente l'estraneità dell'intermediario ai rapporti e alle controversie relative ai beni e/o servizi acquistati. L'intermediario resistente conclude chiedendo all'Arbitro il rigetto del ricorso.

In sede di repliche, parte ricorrente ha precisato che le comunicazioni fornite dall'intermediario sono spesso scarse e confusionarie, posto che quest'ultimo invia frequentemente messaggi promozionali che distolgono l'attenzione del destinatario. Tale circostanza è dimostrata dal fatto che non fosse a conoscenza dell'esistenza del c.d. *"bollino di sicurezza"*. L'intermediario avrebbe dovuto accertarsi che ogni utente fosse informato della possibilità di utilizzare tale servizio, ad esempio evidenziandolo in sede di accesso in app. Avrebbe, altresì, dovuto evitare che i truffatori evidenzino il numero di telefono del *"blocco carte"* per contattare i clienti. Gli eventi occorsi dimostrano pertanto la presenza di lacune nella sicurezza informatica dell'intermediario. Nelle controrepliche, la parte resistente ha richiamato le proprie difese precisando che parte ricorrente non ha fornito, nemmeno in sede di repliche, evidenze concrete in merito ai contatti telefonici truffaldini intercorsi e, dunque, alla dinamica degli eventi oggetto di controversia. Ha poi rappresentato che i Collegi territoriali dell'ABF sono unanimi nel ritenere che la mancata allegazione, da parte del cliente, del messaggio civetta (ovvero, per il *vishing*, del registro delle chiamate) debba determinare il rigetto del ricorso, in quanto non consente di verificare se il mittente/chiamante sia effettivamente riconducibile all'intermediario e, pertanto, se sia idoneo ad ingenerare un legittimo affidamento dell'utente circa la genuinità del messaggio o della telefonata ricevuti. Ha altresì evidenziato che, a differenza di quanto sostenuto dalla parte ricorrente, nei giorni compresi tra il 3/02/2025 e 09/02/2025 – e dunque quando sono avvenuti i fatti oggetto di controversia – nell'applicazione dell'odierna resistente era presente un avviso inerente al presidio del *"bollino di sicurezza"*, visibile a tutti i clienti ad ogni accesso. Infine, ha rappresentato che a seguito delle analisi tecniche dallo stesso condotte non sono emerse evidenze di violazioni dei propri sistemi informatici o eventi riconducibili a fenomeni di *data breach*.

DIRITTO

La controversia verte in materia di esecuzione fraudolenta di transazioni *online*. Più precisamente, l'operazione contestata consiste in una transazione *e-commerce* di €3.485,00,

disposta alle ore 17:41 del 05/02/2025, mediante carta di pagamento di parte ricorrente. L'operazione contestata è disciplinata dal D.Lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.Lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Sulla base della normativa sopra riportata, l'intermediario resistente deve provare, dapprima, l'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute e, in seguito, il dolo o la colpa grave del cliente, uniche ipotesi in cui lo stesso può patire le conseguenze della truffa subita.

Ciò premesso, nel caso in esame, l'intermediario ha riferito e provato con evidenze informatiche che sia l'*enrollment* del dispositivo dei malfattori sia l'operazione contestata sono stati eseguiti mediante i fattori di sicurezza stabiliti dalla *Strong Customer Authentication* (SCA) prevista dalla direttiva (UE) 2015/2366. Infatti, l'accesso da nuovo dispositivo è stato autorizzato attraverso l'inserimento di mail e password di parte ricorrente e del codice dinamico OPT inviato all'utenza telefonica presente in anagrafica cliente, corrispondente a quella di parte ricorrente. In seguito, l'operazione di pagamento è stata autorizzata tramite la notifica *push* giunta sullo smartphone collegato, con un'azione volontaria ("*tap*") eseguita sulla medesima notifica tramite parametro biometrico. A fronte delle evidenze documentali offerte dall'intermediario, il sistema viene ritenuto *compliant* con la SCA e idoneamente provato (Collegio di Torino, decisioni n. 2063/2024; n. 3956/2023; Collegio di Milano, decisione n. 15840/2022).

Assolto quindi l'onere della prova dell'utilizzo di un sistema di sicurezza a due fattori – elemento che costituisce l'antecedente logico rispetto alla prova della colpa grave del cliente – occorre ora esaminare gli elementi della frode e il comportamento di parte ricorrente. Dalla documentazione agli atti e dalle affermazioni rese dalla stessa ricorrente è possibile ricondurre la dinamica della truffa ad un fenomeno di *spoofing*. Alle ore 16.16 del 05/02/2025 parte ricorrente riceveva un sms apparentemente proveniente dall'intermediario, con il quale veniva invitata a contattare il numero mobile ivi indicato in caso di disconoscimento di un'operazione. Contattava tale utenza e collaborava con il sedicente operatore telefonico dell'intermediario resistente comunicando le password ricevute.

Dalla documentazione versata in atti appare dunque chiaro che l'operazione contestata è scaturita da un fenomeno di SMS *spoofing* seguito da *vishing* realizzato ai danni del ricorrente, il quale, dopo aver ricevuto il messaggio civetta, ha contattato il numero ivi indicato, non riconducibile all'intermediario, e ha seguito le indicazioni ricevute da un sedicente operatore dell'intermediario. Tali circostanze portano ad escludere che la responsabilità dell'accaduto possa essere attribuita esclusivamente all'intermediario medesimo, ai sensi della normativa vigente. Pertanto, alla luce delle considerazioni esposte e delle evidenze presenti in atti, il Collegio ritiene sia configurabile un concorso di colpa a carico del ricorrente nella misura del 50% per aver agevolato il compimento della truffa attraverso il contatto diretto al numero indicato nell'sms civetta e non riconducibile all'intermediario.

Pertanto, questo Collegio, valutati tutti i fatti e le circostanze che hanno concorso alla realizzazione della truffa, ritiene che le responsabilità in merito all'operazione fraudolenta debbano essere ripartite fra le parti nella misura del 50%, con il conseguente diritto della parte ricorrente al rimborso della somma di € 1.743,00.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.743,00.

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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

Firmato digitalmente da
EMANUELE CESARE LUCCHINI GUASTALLA