Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) CAPIZZI

Seduta del 02/09/2025

FATTO

Con ricorso del 29 aprile 2025, la ricorrente riferisce di avere denunciato, in data 22 gennaio 2025, con successiva integrazione del 23 gennaio 2025, di essere stata oggetto di frode informatica – asseritamente riconducibile al fenomeno c.d. phishing tramite ricezione di telefonate (vishing) e successivo invio di sms truffaldini (smishing) – che si sarebbe concretizzata nell'esecuzione, il medesimo 22 gennaio 2025, di n. 2 (due) bonifici istantanei, per un importo complessivo pari a € 14.500,00.
Le suddette transazioni sono state realizzate tramite accesso in App all'area riservata dei servizi di mobile banking dell'intermediario sul device certificato della cliente. Di conseguenza, disconoscendo gli addebiti registrati sul proprio conto corrente relativamente alle operazioni sopra evidenziate, in quanto frutto di frode informatica, e inputando la responsabilità della suddetta frode all'intermediario convenuto, il quale non avrebbe saputo impedire una violazione al proprio sistema informatico da parte dei truffatori, la ricorrente ha chiesto il rimborso della somma complessiva di € 14.500,00 relativa alle menzionate operazioni di pagamento contestate e disconosciute.
L'intermediario convenuto, con le controdeduzioni, sostiene la regolare contabilizzazione, autenticazione e registrazione dell'operazione in oggetto, evidenziando inoltre la colpa grave della cliente che, oltre a non avere fornito una descrizione circostanziata della truffa, ha collaborato, sia pure inconsapevolmente, all'esecuzione del pagamento contestato. Chiede dunque il rigetto del ricorso.

DIRITTO

La questione sottoposta al Collegio concerne la rimborsabilità o meno in favore di parte ricorrente della somma fraudolentemente sottratta mediante svolgimento di operazioni disconosciute.
Si tratta, in particolare, di n. 2 (due) bonifici istantanei, per un importo complessivo pari a € 14.500,00, eseguiti tre le ore 14:46 e le ore 14:48 del giorno 22 gennaio 2025. Le suddette operazioni sono state eseguite tramite accesso in App, su device precedentemente registrato dalla cliente, all'area riservata dei servizi di mobile banking dell'intermediario.
Alla data di effettuazione delle operazioni contestate era vigente il D. Lgs. n. 11/2010, modificato a seguito dell'entrata in vigore del D. Lgs. n. 218/2017 di recepimento della direttiva (UE) 2015/2366 (c.d. PSD II). Pertanto, la sussistenza delle responsabilità che le parti della controversia odierna vicendevolmente si addebitano dovrà essere valutata in base a quanto previsto da tale decreto con riferimento a entrambi i profili caratterizzanti l'onere probatorio, ossia l'accertamento della regolare autenticazione ed esecuzione delle operazioni di pagamento, nonché l'accertamento dell'eventuale colpa grave dell'utilizzatore dei servizi di pagamento.
Con riferimento al primo profilo, il Collegio osserva che l'art. 8, comma 1, lett. a) del D. Lgs. 11/2010, come novellato dal D. Lgs. 218/2017, prevede che "*il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: a) assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7* […]".
L'art. 10, comma 1, del medesimo Decreto prescrive che "*qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*".
L'art. 10, comma 2, prevede che "*quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita*, […] *è onere del prestatore di servizi di pagamento* […] *fornire la prova della frode, del dolo o della colpa grave dell'utente*".
Inoltre, con riferimento alle modalità di autenticazione di una operazione di pagamento, ai sensi dell'art. 10 bis, comma 1, "*i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*".
L'art. 1, comma 1, lett. q-bis, del summenzionato testo normativo definisce l' "autenticazione forte del cliente" quale "*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*".
Vale comunque la pena ribadire che, già prima dell'entrata in vigore delle citate modifiche normative, l'orientamento consolidato dei Collegi ABF era nel senso di richiedere all'intermediario la prova dell'avvenuta autenticazione delle operazioni tramite sistema a due o più fattori (cfr. ex multis Collegio di Milano, Decisioni n. 6936/2016 e n. 7131/2017).

Quanto al secondo profilo dell'onere probatorio, l'orientamento consolidato dell'Arbitro è nel senso conformarsi al principio interpretativo statuito dal Collegio di Coordinamento (Decisione n. 22745/2019), secondo cui "*la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente*".

Tuttavia, il Collegio di Coordinamento ha al contempo evidenziato che, anche "*nel caso in cui l'intermediario si sia costituito nel procedimento, fornendo prova dell'autenticazione e della regolarità formale dell'operazione, ma nulla abbia dedotto in merito alla colpa grave dell'utente, il Collegio [può] comunque affermarne l'accertamento se palesemente emergente dalle dichiarazioni rese dal ricorrente in sede di denuncia all'autorità giudiziaria e/o nel ricorso*".

Venendo ora al caso di specie, si rileva, innanzitutto, che dalla ricostruzione dei fatti presente nella documentazione versata in atti, con particolare riferimento alla denuncia sporta alle competenti autorità giudiziarie, non è possibile appurare con precisione la dinamica della truffa asseritamente perpetrata ai danni di parte ricorrente, salvo desumere che la cliente sia caduta vittima del noto fenomeno del c.d. "phishing attraverso vishing/smishing", realizzato mediante iniziale ricezione di una telefonata truffaldina apparentemente proveniente da un operatore del servizio antifrode della banca, che informava la medesima della necessità di disinstallare dal proprio device l'App dei servizi di mobile banking della banca a causa di alcuni accessi anomali riscontrati, a seguito dei quali si erano registrate due operazioni di pagamento fraudolente.

L'intermediario convenuto, attraverso le evidenze versate in atti e i log prodotti, ricostruisce i singoli passaggi dell'esecuzione dei bonifici istantanei di cui è ricorso e dimostra che la fase antecedente all'esecuzione dell'operazione contestata è stata autenticata attraverso il sistema autorizzativo di tipo dinamico funzionante mediante digitazione delle credenziali statiche (fattore della conoscenza) – codice cliente, data di nascita e codice PIN – e codice Token generato in App sul device certificato della cliente (fattore del possesso).

Una ulteriore attività prodromica all'esecuzione dei pagamenti di cui è ricorso è consistita nell'effettuazione di un giroconto di importo pari a € 14.000,00 dal conto deposito al conto corrente intestato alla cliente.

Tuttavia, trattandosi di una operazione strumentale alla costituzione della provvista, in conformità a quanto stabilito dal Collegio di Coordinamento con Decisione n. 8671/2024, la medesima è sottratta dall'obbligo della prova di autenticazione forte a due fattori (Strong Customer Authentication – SCA).

Con riferimento, infine, all'esecuzione dei pagamenti online contestati, il convenuto produce evidenza dell'inserimento del codice Token generato in App sul device certificato della ricorrente (fattore del possesso).

Al riguardo, pur se non chiaramente esplicitato dal convenuto, dalla documentazione versata in atti e dall'analisi della cronologia degli accadimenti, è lecito supporre che i codici Token necessari per l'autenticazione delle operazioni di pagamento siano stati generati nella medesima sessione di accesso all'area riservata della cliente precedentemente autorizzata tramite SCA. Ragion per cui si può ritenere, in conformità con quanto chiarito dall'EBA (cfr. Q&A EBA ID 2018_4141), che il fattore della conoscenza costituito dall'inserimento delle credenziali statiche sopra citate possa validamente costituire il primo fattore di autenticazione anche per tali operazioni (cfr. ex multis Collegio di Milano, Decisioni n. 1212/2025 e n. 9002/2024).

Alla luce delle evidenze in atti, questo Collegio conclude che il sistema predisposto dall'intermediario è conforme ai criteri previsti per l'autenticazione forte a "due fattori", il che, in conformità con l'orientamento consolidato dell'Arbitro, induce a ritenere, in assenza di ulteriori indici di anomalia delle operazioni contestate, che parte resistente abbia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 del D. Lgs. n. 11/2010, (cfr. ex multis Collegio di Milano, Decisioni n. 10279/2024, n, 8996/2024 e n. 7703/2024).

È ora possibile passare alla disamina circa l'assolvimento da parte del convenuto dell'onere probatorio in merito alla colpa grave dell'utente del servizio di pagamento.

Sul punto, dalla ricostruzione dei fatti così come evincibile dalla documentazione versata in atti dalle parti, pare sia da escludersi, nella vicenda in oggetto, la possibilità di desumere in capo all'utilizzatore un comportamento gravemente colposo, non essendo presente una serie di elementi di fatto particolarmente univoca e convergente, al punto che possa ragionevolmente ritenersi che l'utilizzo fraudolento sia effettivamente riconducibile sul piano causale alla condotta dell'utilizzatore (cfr. ex multis Collegio di Roma, Decisione n. 6770/2022; Collegio di Milano, Decisioni n. 7844/2021 e n. 1828/20).

Al proposito, occorre ricordare che, secondo quanto indicato dalla giurisprudenza di legittimità (cfr. Cass. civ., 19 novembre 2001, n. 14456) e dal Collegio di Coordinamento (Decisione n. 5304/2013), la colpa grave consiste in "*un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti*".

Invero, nella vicenda al centro della presente controversia, il Collegio ritiene che la responsabilità della cliente sia temperata dalla natura particolarmente insidiosa e sofisticata della truffa di cui è ricorso, realizzatasi attraverso "ID caller spoofing" mista a un tradizionale smishing. In effetti, come risultante dalla denuncia e dal registro chiamate prodotto in atti, il numero telefonico utilizzato alle ore 14:32 del 22 gennaio 2025 ai fini della perpetrazione della truffa al centro della presente controversia appare riferibile al servizio "Aiuto e Supporto" indicato nella pagina web dell'intermediario: e ciò non può essere senza conseguenze in quanto l'apparente provenienza da un canale ufficiale dell'intermediario può senz'altro attenuare il livello di attenzione e di sospetto da parte del cliente (cfr. ex multis Collegio di Milano, Decisione n. 4033/2021).

Quanto, invece, agli sms truffaldini ricevuti dalla cliente, non vi sono elementi nel caso di specie, in relazione alle allegazioni prodotte dalla cliente, che consentano di ricondurre la truffa alla più sofisticata e insidiosa fattispecie nota come "sms spoofing". Gli sms prodotti, infatti, a prescindere dalla veridicità e correttezza del loro contenuto, riportando delle date molto distanti temporalmente dagli accadimenti di cui è ricorso, non possono in alcun modo essere ricollegabili alla truffa in questione.

Ciò considerato, in relazione alla fattispecie di truffa oggetto della presente controversia, i Collegi sono unanimi nel ritenere che non sia generalmente ravvisabile la colpa grave della ricorrente, a meno che non si rinvengano degli indici di inattendibilità o anomalia della telefonata truffaldina; in tale caso, potrà essere ravvisato un concorso di colpa tra le parti 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 riscontrate criticità organizzative del servizio di pagamento offerto in via fisiologica dall'intermediario (cfr. ex multis Collegio di Milano, Decisione n. 22674/2021; Collegio di Roma, Decisione n. 21696/2020; Collegio di Coordinamento, Decisione n. 22745/2019).

Pertanto, il Collegio, in conformità all'orientamento consolidato dell'Arbitro, da cui non c'è ragione di discostarsi, valutata la gravità delle colpe a carico di entrambe le parti in

relazione ai fatti illustrati e documentati, ritiene dunque di doverle ripartire in misura di metà a carico della parte ricorrente e di metà a carico della parte resistente, con la conseguenza che l'intermediario dovrà provvedere a corrispondere al cliente la somma di € 7.250,00, pari al 50% della somma fraudolentemente sottratta (cfr. ex multis Collegio di Milano, Decisioni n. 8435/2023, n. 3819/2023 e n. 2184/2023).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 7.250,00.
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.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TINA