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 9 maggio 2025, la ricorrente riferisce di avere denunciato, in data 17 marzo 2025, di essere stata oggetto di frode informatica – asseritamente riconducibile al fenomeno c.d. phishing tramite telefonata truffaldina (vishing) e successiva ricezione di sms (smishing) – che si sarebbe concretizzata nell'esecuzione, il precedente 8 marzo 2025, di un pagamento online di importo pari a € 315,00, tramite carta di debito intestata alla medesima ed emessa dall'intermediario convenuto.
La suddetta transazione è stata realizzata tramite accesso via web all'area riservata dei servizi di internet banking dell'intermediario. Di conseguenza, disconoscendo gli addebiti registrati sul proprio conto corrente relativamente all'operazione sopra evidenziata, 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 di € 315,00 relativa alla menzionata operazione di pagamento contestata e disconosciuta.
Chiede inoltre: (i) la verifica della "sicurezza dei sistemi bancari" del convenuto, (ii) l'avvio di una indagine sulla "filtrazione" dei dati personali riferiti alla medesima; (iii) un

risarcimento a compensazione del "danno emotivo" procurato, (iv) il rafforzamento a cura della banca delle proprie "politiche di protezione dei dati", e (v) "che venga garantita una migliore tutela per i clienti".
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, per sua stessa ammissione, ha cooperato attivamente all'esecuzione del pagamento contestato seguendo le indicazioni ricevute telefonicamente dai truffatori, pur provenendo da un'utenza non riconducibile alla banca.
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 un'operazione disconosciuta. Si tratta, in particolare, di un pagamento online con carta di debito intestata alla cliente, di importo pari a € 315,00, eseguito alle ore 11:06 del giorno 8 marzo 2025. La suddetta operazione è stata eseguita tramite accesso via web all'area riservata dei servizi di internet banking dell'intermediario.
Il Collegio rileva innanzitutto come, dall'analisi della documentazione versata in atti, con riferimento alla dinamica della truffa di cui è ricorso, non è contestata la circostanza che la ricorrente dichiari chiaramente di aver dato seguito, almeno parzialmente, alle indicazioni ricevute telefonicamente da un sedicente operatore dell'intermediario, collaborando dunque con il truffatore per l'esecuzione del pagamento di cui è ricorso.
Senonché, dalla documentazione versata in atti e dai log prodotti, è pacifico rilevare che: a) la ricorrente, eseguendo le indicazioni fornite dal sedicente operatore della banca, che segnalava indebiti accessi all'area riservata dei servizi di internet banking della banca, ha fornito le credenziali statiche necessarie per l'accesso all'area personale; b) l'operazione di pagamento al centro della presente controversia è stata autorizzata tramite la condivisione con il truffatore di un codice OTP ricevuto via sms sul device certificato della cliente, la quale pensava servisse invece a bloccare la carta di debito di cui è ricorso.
In proposito, si ritiene che se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad esempio con l'inserimento, come nel caso di specie, di uno solo dei fattori di autenticazione), l'operazione contestata non deve intendersi, per ciò solo, autorizzata (cfr. Collegio di Milano, Decisione n. 4601/2024).
Ne consegue che, in relazione alla data di effettuazione delle operazioni contestate, la sussistenza delle responsabilità che le parti della controversia odierna vicendevolmente si addebitano dovrà essere valutata in base a quanto previsto dal vigente 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) 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 parrebbe che la cliente sia caduta vittima del noto fenomeno del c.d. "phishing attraverso vishing misto a smishing", realizzato mediante iniziale ricezione di una telefonata truffaldina apparentemente proveniente da un'utenza telefonica riconducibile alla banca, nella quale un ignoto truffatore, che si qualificava come un operatore dell'intermediario convenuto, induceva la cliente ad attivare apposita procedura atta a prevenire indebiti accessi alla propria area riservata dei servizi di internet banking dell'intermediario.
Conseguentemente, la cliente, seguendo le istruzioni del sedicente operatore, provvedeva all'inserimento dei fattori di autenticazione necessari per consentire ai truffatori di accedere alla propria area riservata e, quindi, eseguire il pagamento di cui è ricorso.

L'intermediario convenuto, attraverso le evidenze versate in atti, riferisce che, in termini generali, sia la procedura di accesso all'area riservata dei servizi di mobile banking offerti alla clientela, sia la procedura dispositiva per l'esecuzione dell'operazione di pagamento sono pienamente conformi rispetto al sistema di autenticazione forte a due fattori (Strong Customer Authentication – SCA) con corretta applicazione della tecnologia 3D Secure ("3DS"), che prevede l'inserimento delle credenziali statiche, ossia username e password (fattore della conoscenza), unitamente all'utilizzo delle credenziali dinamiche, ossia il codice monouso OTP inviato tramite sms sul device certificato dell'utilizzatore (fattore del possesso) o, in alternativa, l'attivazione tramite riconoscimento biometrico di un token generato in App su smartphone precedentemente registrato (fattore della inerenza).
Tuttavia, l'intermediario precisa anche la propria scelta di avvalersi dell'esenzione dalla SCA prevista dall'art. 10 del Regolamento delegato (UE) 2018/389, che consente che l'accesso al conto per fini meramente informativi possa avvenire senza applicare la SCA, a condizione che non siano decorsi più di 180 giorni dall'ultima applicazione della SCA. Ed effettivamente, il Collegio, dall'analisi dei log prodotti e versati in atti, osserva che, con riferimento alla fase di accesso all'area riservata per la fruizione dei servizi di internet banking prodromico alla generazione del CVV dinamico, si ha evidenza soltanto del fattore di conoscenza (digitazione di username e password), ma non di quelli di possesso (invio del codice monouso OTP tramite sms) o di inerenza (riconoscimento tramite biometria), cui lo stesso intermediario ha fatto in precedenza riferimento.
Tenendo conto di quanto previsto, in tema di SCA, dalle "Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2", si deve concludere che l'intermediario intervenuto ha fallito nell'offrire prova di corretta autenticazione forte con riferimento alla fase di login prodromica all'esecuzione dell'operazione contestata, in quanto non è stata prodotta chiara e completa evidenza in merito ai requisiti di autenticazione previsti dal richiamato D. Lgs.11/2010 (cfr. ex multis Collegio di Milano, Decisioni n. 7792/2024, n. 4951/2023 e n. 6642/2023).
Né il Collegio ritiene possa essere condivisa l'argomentazione di parte resistente relativa all'esenzione dalla SCA prevista dall'art. 10 del richiamato Regolamento delegato (UE) 2018/389: la disposizione in esame, infatti, limita l'esenzione della SCA solo ad accessi di tipo meramente informativo (e non dispositivo come nella specie).
Essendo provato (ed anzi dichiarato dallo stesso intermediario) che l'accesso prodromico all'operazione disconosciuta non è stato effettuato mediante SCA, il ricorso non può che essere accolto, essendo principio pacifico, in aderenza al dato normativo, che la prova dell'autenticazione forte rappresenta un antecedente logico rispetto alla prova della colpa grave dell'utente.
Il che, appunto, esime sia dall'esame della prova della sussistenza della SCA in relazione al pagamento online contestato, sia dall'accertamento dell'eventuale colpa grave di parte ricorrente (cfr. ex multis Collegio di Milano, Decisioni n. 10636/2024, n. 8155/2024 e n. 7574/2024).
Ne consegue che l'operazione di pagamento disconosciuta al centro della presente controversia dovrà essere rimborsata per intero dall'intermediario convenuto, nei limiti già precisati dell'importo chiesto dalla cliente in sede di ricorso.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 315,00.

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