COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) CAPIZZI

Seduta del 28/04/2025

FATTO

Il ricorrente riferisce di avere denunciato in data 23 luglio 2024 di essere stato oggetto, il medesimo giorno, di frode informatica, che si sarebbe concretizzata nell'addebito sul rapporto di conto corrente intrattenuto presso l'intermediario convenuto di un bonifico ordinario, di importo pari a € 7.000,00. La menzionata operazione di pagamento è stata disposta tramite accesso in App sul *device* registrato del cliente all'area riservata dei servizi di mobile banking dell'intermediario. Il ricorrente precisa, inoltre, di essersi accorto tempestivamente della frode e di aver chiesto alla banca, sempre in data 23 luglio 2024, la revoca del bonifico, senza tuttavia ottenere l'esito auspicato. Di conseguenza, disconoscendo l'addebito registrato sul proprio conto corrente sopra evidenziato, in quanto frutto di frode informatica, e inputando la responsabilità della suddetta frode all'intermediario, che non avrebbe saputo impedire una violazione al proprio sistema informatico da parte dei truffatori, il ricorrente ha chiesto il rimborso della somma complessiva di € 7.000,00 relativa alla menzionata operazione di pagamento on-line contestata e disconosciuta.

L'intermediario, con le controdeduzioni, sostiene la sua regolare esecuzione dell'operazione in oggetto a seguito del corretto inserimento delle credenziali previste nell'ambito del sistema adottato di autenticazione forte (SCA) ai fini sia dell'accesso all'area riservata per l'utilizzo dei servizi di mobile banking del convenuto, sia

dell'inserimento della disposizione di pagamento contestata, e chiede dunque il rigetto del ricorso. Sostiene, in particolare, la non revocabilità del bonifico contestato in conformità a quanto previsto dall'articolo 17 del D. Lgs. n. 11/2010 in tema di irrevocabilità degli ordini di pagamento. Eccepisce preliminarmente l'inammissibilità del ricorso per mancanza del preventivo reclamo.

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 di pagamento disconosciuta.

In via preliminare, il Collegio è chiamato a esprimersi in merito all'eccezione nel rito sollevata dalla banca convenuta, la quale chiede sia dichiarata l'improcedibilità del ricorso stante la mancata presentazione del preventivo reclamo da parte del cliente. L'eccezione non coglie nel segno. Come noto, le nuove "*Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari*" (c.d. "Disposizioni ABF"), applicabili ai ricorsi presentati dal primo ottobre 2020, dopo aver definito come reclamo "*ogni atto con cui un cliente chiaramente identificabile contesta in forma scritta (es., lettera, fax, e-mail) all'intermediario un suo comportamento anche omissivo*", precisano che "*il ricorso all'ABF è preceduto da un reclamo preventivo all'intermediario*" e che "*il cliente rimasto insoddisfatto o il cui reclamo non abbia avuto esito nel termine di 60 giorni dalla sua ricezione da parte dell'intermediario può presentare proposto ricorso all'Arbitro Bancario Finanziario*" (Sez. VI, par. 1).

Il reclamo costituisce, dunque, una condizione di procedibilità ai fini del valido esperimento della procedura ABF, sicché la sua mancanza, integrando l'inesistenza di un presupposto dell'azione, può, tra l'altro, essere rilevata anche d'ufficio dall'Arbitro (cfr. ex multis Collegio di Milano, Decisioni n. 25181/2021 e n. 19463/2020; Collegio di Coordinamento, Decisioni n. 15400/2021 e n. 5304/2013). Nel caso di specie, tuttavia, dalla documentazione versata in atti, il Collegio rileva come il cliente abbia trasmesso via e-mail all'intermediario in data 23 luglio 2024 – il giorno in cui è stata eseguito il pagamento fraudolento di cui è ricorso – la denuncia alle autorità estere dove si trovava al momento della truffa, e la collegata integrazione, a supporto dell'istanza di revoca del bonifico di cui è ricorso. Ebbene, poiché la suddetta e-mail, ad avviso del Collegio, costituisce *de facto* formale disconoscimento dell'operazione contestata e, conseguentemente, sulla base del consolidato orientamento dell'Arbitro, assume valenza di preventivo reclamo, l'eccezione dell'intermediario non può trovare accoglimento (cfr. ex multis Collegio di Milano, Decisioni n. 8117/2024, n. 22614/2023, n. 15485/2022 e n. 5458/2022).

Il Collegio passa quindi ad esaminare il merito della controversia, al centro della quale vi è un bonifico ordinario, di importo pari a € 7.000,00, eseguito tra le ore 01:44 e le ore 01:51 del 23 luglio 2024. L'operazione contestata è stata eseguita tramite accesso in App, su *device* certificato del cliente, all'area riservata dei servizi di mobile banking dell'intermediario resistente. 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 autorità estere dove il cliente si trovava al momento del fatto, non è possibile appurare con precisione la dinamica della truffa asseritamente perpetrata ai danni di parte ricorrente, salvo desumere che il cliente ritiene che l'operazione di pagamento contestata sia stata disposta e autorizzata dal proprio telefono cellulare contro la propria volontà, in quanto asseritamente dormiente al momento di esecuzione della stessa.

L'intermediario, 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 delle operazioni 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 in App sul device certificato dell'utilizzatore all'area riservata per la fruizione dei servizi di mobile banking, si ha evidenza soltanto del fattore di inerenza (riconoscimento), ma non di quelli di possesso (invio del codice monouso OTP tramite SMS) o di conoscenza (username e password), cui lo stesso ha fatto 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 (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 dal cliente in sede di ricorso.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 7.000,00.
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