

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) MODICA

Seduta del 17/03/2026

FATTO

La cliente afferma che, alle ore 11:41 del 15/01/2025, contattava telefonicamente il servizio clienti della banca per richiedere alcune informazioni sul proprio c/c; una voce automatica la invitava a comunicare il proprio recapito telefonico per essere richiamata da un operatore; alle ore 17:14 riceveva una chiamata dallo stesso servizio clienti, con la quale veniva avvertita di un bonifico di € 4.000,00 in favore di soggetto a lei sconosciuto. L'operatore le comunicava che avrebbe potuto recuperare la somma purché avesse trasferito tutto il danaro depositato presso il cc su un diverso cc; si avvedeva che qualcuno dall'esterno e senza il suo consenso (es. un hacker) riusciva a muovere il cursore del proprio computer e, pertanto, comunicava all'operatore che avrebbe, prima, avvisato la Polizia di quanto stava accadendo; riattaccava e riceveva, immediatamente dopo, una chiamata dal n. *61 da un interlocutore che si presentava come Agente di Polizia di Milano e comunicava che la Polizia era già al corrente di quanto stava accadendo, confermando la necessità di trasferire il danaro su di un altro cc; riattaccava il telefono non rispondendo più alle numerose chiamate ulteriormente ricevute dal numero *89. Da una successiva verifica dell'estratto conto, scopriva che, oltre alla disposizione di bonifico fraudolenta era stata trasferita la somma di € 46.389,88 dal c/c ad un secondo c/c, il solo dal quale era possibile effettuare bonifici; in data 16/01/2025 provvedeva a disconoscere l'operazione e sporgeva denuncia.

Lamenta che l'operazione presentava molteplici "red flags" (primo pagamento a beneficiario mai utilizzato, bonifico istantaneo, importo non ricorrente, contesto di chiamate fraudolente immediatamente precedenti, possibile trasferimento interno propedeutico), che imponevano alert/blocchi o step-up authentication.

Chiede la restituzione di € 4.000,00, oltre al risarcimento del danno extracontrattuale e la refusione delle spese legali.

L'intermediario controdeduce che le operazioni disconosciute risultano eseguite senza anomalie e personalmente dalla ricorrente, seguendo le istruzioni fornite al telefono da un soggetto che si era qualificato come incaricato della Banca; il giorno 15/01/2025 è stato effettuato un accesso nell'Area Riservata web della cliente e sono stati predisposti 2 bonifici (l'operazione contestata da € 4.000,00 ed un giroconto di € 46.000,00). Le operazioni sono state autorizzate tramite SCA, utilizzando il fattore di conoscenza (codice utente e pin) e del possesso (lo smartphone, del quale solo il cliente è in possesso); specifica che l'app è installata sul dispositivo mobile (samsung_SM-A*), sul quale è attivo il Servizio Token, di esclusiva disponibilità della cliente in quanto è lo stesso device utilizzato in fase di attivazione del Token in data 15/05/2024; sullo smartphone è stata inviata una notifica push autorizzativa per l'accesso da web, nonché il codice operazione temporaneo generato offline dall'app per l'operazione di bonifico. Sostiene che vi sia sussistenza di colpa grave della parte ricorrente, che ha dimostrato una condotta gravemente sprovveduta e colposa, in quanto, usando l'ordinaria diligenza, la stessa avrebbe potuto accorgersi dell'inganno in corso, o comunque insospettirsi nel corso del suo evolversi.

Chiede il rigetto del ricorso.

La cliente replica che: il secondo numero dal quale ha ricevuto una chiamata (*61) non è riportato in denuncia come recapito della banca, ma riconducibile ad un operatore di Polizia; la denuncia non contiene alcuna ammissione di "cooperazione"; manca la prova di consenso a qualunque controllo remoto e di comunicazione di codici. Evidenzia la mancanza dell'autenticazione da cellulare: la notifica push per il bonifico non viene consegnata e l'operazione viene portata a termine interamente sul PC tramite il percorso offline/fallback. In questo flusso, il Codice Operazione viene mostrato sullo schermo del PC, la App viene usata al più come generatore passivo (senza mostrare all'utente i dati essenziali dell'ordine) e il Codice Token viene reimmesso sul PC per confermare; ne consegue che il cellulare non svolge la funzione di canale autorizzativo in senso PSD2 (niente push, niente dynamic linking sul device), mentre tutto ciò che decide — challenge, conferma e completamento — avviene nel perimetro del PC.

DIRITTO

La cliente disconosce un bonifico eseguito a valle di una truffa e chiede la restituzione del relativo importo, pari a 4.000,00 euro.

Diversamente da quanto rappresentato dall'intermediario nelle controdeduzioni, la cliente, in sede di denuncia, non dichiara di avere condiviso lo schermo con il truffatore, sicché l'operazione, effettuata alle ore 17:55 del 15/01/2025, ricade nel raggio d'azione del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2). Ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010, "Qualora l'utilizzatore 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'assolvimento di tale onere è necessario ma non sufficiente, dovendo il prestatore ulteriormente

provare, ai fini dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010: come chiarito dal Collegio di Coordinamento, "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" (decisione n. 22745/2019).

Il Collegio, richiamati gli artt. 97 e 98 della PDS2, l'articolo 10 bis del D. Lgs. 11/2010, le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare il parere dell'EBA del 21 giugno 2019), richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento": "Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Il Collegio, ancora, ricorda che, in base all'art. 1, lett. qbis, l'"autenticazione forte del cliente" è definita come "un'autenticazione 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". L'autenticazione forte è richiesta nella fase di accesso al conto/enrollment dell'app/registrazione della carta sul wallet; nella fase di esecuzione delle singole operazioni; rispetto a qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Nel caso di specie, l'intermediario ha fornito prova di autenticazione con impiego di doppio fattore. Con riguardo alla fase preliminare all'operazione, risulta che i fattori di autenticazione impiegati per l'accesso in app e sul sito web sono il Codice Smartc* (e pin), quale elemento di conoscenza e il device sul quale è stata installata l'app (token app), quale elemento di possesso. Con riferimento all'operazione contestata, dai log allegati risulta che la cliente ha fatto accesso alla pagina "bonifici" e predisposto il bonifico; ha inserito i dati del bonifico (importo, causale, IBAN e Denominazione del beneficiario) e confermato l'operazione facendo click sul bottone "Avanti": alle ore 17:51:10 l'intermediario ha effettuato i controlli sulla validità dei dati inseriti. Avendo il bonifico superato i controlli previsti, viene mostrata la pagina di riepilogo dei dati con la richiesta di autorizzazione e il cliente chiede di autorizzare l'operazione facendo click sul bottone "Avanti"; l'intermediario effettua i controlli per stabilire le modalità di autorizzazione dell'operazione e alle ore 17:51:32 prepara la PUSH per autorizzare il bonifico (numero 161761951). Il cliente non riceve la PUSH e quindi ricorre alla autorizzazione con la generazione di un Codice Operazione temporaneo, che appare sullo schermo del PC; digita il codice sulla App e conferma. A questo punto, sulla App viene generato un Codice Token che il cliente inserisce nella apposita voce della schermata del PC e conferma facendo click sul bottone "Continua". Al termine, viene mostrata al cliente la pagina di conferma. Risulta inviata una notifica e-mail all'indirizzo della cliente alle ore 17:55. Alla luce dei dati forniti dall'intermediario, reputa questo Collegio che la SCA risulti provata mediante Codice Operazione e Codice Token generato dalla app, che, secondo gli orientamenti dei Collegi ABF, sono elemento di possesso; riutilizzo del PIN della fase di login, considerato che il login è delle ore 17:44 e il bonifico delle ore 17:55, dunque "within a matter of minutes within the same session", secondo le indicazioni fornite dall'EBA (https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4141).

Del pari provata appare la colpa grave della cliente, vittima di una truffa banale cui avrebbe potuto sottrarsi con l'impiego di una media diligenza. Al di là della circostanza che il numero 02***6789 che la cliente dichiara di avere spontaneamente contattato per prendere informazioni in merito al proprio c/c

non coincide perfettamente col numero ufficiale dell'intermediario, che contiene anche il prefisso +39, è la complessiva dinamica della frode a presentare caratteri evidenti di grossolanità. Alla luce delle specificità del caso concreto, ritiene il Collegio che risulti provata non solo l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione nonché la sua regolarità formale, ma anche dimostrata la colpa grave di parte ricorrente (cfr. in proposito Collegio di Coordinamento, decisione n. 22745/2019), in quanto le modalità attuative delle operazioni disconosciute riflettono uno schema tipico e ormai noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, sms o altri strumenti, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza. Tenuto conto delle circostanze del caso, la ricorrente deve essere considerato vittima di colpevole credulità, in quanto le modalità con le quali la truffa è stata realizzata rientrano tra quelle più diffuse e conosciute, che qualunque fruitore di servizi on line, dotato di normale avvedutezza e prudenza, deve essere in grado di riconoscere ed evitare (cfr. Collegio di Coordinamento n. 3498 del 26/10/2012).

La riconosciuta colpa grave del cliente, pur a fronte di operazioni accompagnate da piena prova della Sca, non esclude naturalmente che il Collegio, tenuto conto delle peculiarità della vicenda, possa individuare altri e diversi eventuali profili di responsabilità, per esempio sul versante del rispetto degli obblighi di protezione che gravano, per diritto comune, sul *bonus argentarius* anche *sub specie* di mancata gestione di eventi che segnalino la possibilità di frodi o anomalie; profili che, nella vicenda in esame, non ricorrono.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE