COLLEGIO DI MILANO

composto dai signori:

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

Relatore FRANCESCA DELL'ANNA MISURALE

Seduta del 13/02/2025

FATTO

Con ricorso del 19/11/2024, il cliente espone quanto segue:

- subiva una frode telefonica ricevendo una telefonata dal numero verde dell'intermediario;
- durante la chiamata, un sedicente operatore della banca la informava di una presunta attività fraudolenta all'estero, a valere sulla propria carta di pagamento;
- l'interlocutore dichiarava di procedere al blocco di tali pagamenti e chiedeva che gli venissero forniti alcuni codici via SMS;
- poco dopo riceveva la notifica dell'avvenuta esecuzione di un bonifico di € 9.900,00;
- resasi conto della truffa, contattava l'intermediario chiedendo il blocco del bonifico e presentava denuncia alle competenti Autorità.

Pertanto, chiede, il rimborso di € 9.900,00.

L'intermediario afferma quanto segue:

- la richiesta di rimborso della cliente è del tutto infondata, come già era stato evidenziato nel precedente procedimento, dichiarato inammissibile dal Collegio di Milano per difetto di preventivo reclamo;
- l'operazione è stata correttamente contabilizzata, registrata e autenticata in quanto attuata con il corretto inserimento delle credenziali, tanto in fase di accesso al conto, quanto in fase dispositiva;

- la cliente ha fornito incautamente collaborazione ai truffatori, comunicando loro i codici OTP necessari a finalizzare la procedura di cambio password, quanto la richiesta di bonifico;
- sussiste la colpa grave della cliente, in violazione dei propri obblighi ai sensi dell'art. 7 del D.lgs. 11/2020;
- quanto allo schema fraudolento, esso è riconducibile al cosiddetto *vishing*, laddove è oramai fatto notorio che i numeri verdi sono abilitati esclusivamente alla ricezione delle chiamate, e non anche al loro inoltro;
- l'intermediario ha diffuso apposite campagne informative volte a sensibilizzare la clientela rispetto alle forme più diffuse di frode.

Pertanto, l'intermediario chiede il rigetto del ricorso.

La cliente ribadisce i profili di responsabilità ascritti all'intermediario, eccependo in via ulteriore che:

- la chiamata appariva provenire da un contatto ufficiale della banca, i cui sistemi informatici sono stati evidentemente compromessi dall'attività dei frodatori;
- le prospettazioni della resistente circa i presidi di sicurezza della procedura di cambio password sono contraddittorie, dal momento che la stessa ha dichiarato che dopo numerosi tentativi di cambio password, effettuati nel giro di pochi minuti, il sistema riconosceva come genuino il tentativo di accesso;
- i sistemi di sicurezza avrebbero dovuto intercettare una tale operatività anomala, e avrebbero dovuto richiedere una chiamata di sicurezza alla cliente, dal momento che la stessa ignorava che i codici OTP che forniva al falso operatore erano necessari ad effettuare il cambio password;
- il beneficiario del bonifico è un cliente della stessa banca resistente.

In sede di controrepliche l'intermediario rileva che non può essere ricondotta a responsabilità della banca la circostanza che i frodatori possano adottare modalità tecniche, oramai di ampia diffusione e notorietà, che sono in grado di camuffare il vero mittente di chiamate e SMS, facendo apparire come tale un contatto della banca. Ribadisce, infine, le circostanze da cui trarre la responsabilità per colpa grave della cliente e l'infondatezza del ricorso.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di un bonifico di € 9.900,00 eseguito in data 15/01/2024, alle ore 18:51.
È in atti la denuncia presentata dalla cliente il 03/02/2024.

La disciplina da applicarsi alla fattispecie è quella dettata dal D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218 di recepimento della Direttiva 2015/2366 UE relativa ai servizi di pagamento nel mercato interno (cosiddetta PSD2) in vigore dal 13/01/2018. Segnatamente, la *strong customer authentication* (cosiddetta SCA) è disciplinata dagli artt. 97 e 98 della PSD2, dall'art. 10-bis del D.lgs. 11/2010, dalle 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 dai criteri interpretativi forniti dall'EBA, in particolare dal parere dell'EBA del 21 giugno 2019.

Con particolare riferimento all'autenticazione forte richiesta per tutte le operazioni online a far data dal 14 settembre 2019, deve ricordarsi che questa è richiesta quando il cliente: 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.
La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza e possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.
Al riguardo, giova precisare che l'art. 10 del D.lgs. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione 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; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto (sull'onere probatorio riguardante l'autenticazione forte e la condotta gravemente colposa del cliente in capo all'intermediario cfr. Collegio di Coordinamento, decisione n. 22745 del 10 ottobre 2019).

Per quanto attiene all'autenticazione forte, l'intermediario afferma che l'operazione contestata è stata correttamente contabilizzata, registrata e autenticata.
Sta di fatto che dalla documentazione (log e relative legende) versate in atti dall'intermediario non è dato ricavare la piena prova della SCA.
In particolare, per quanto attiene alla fase di accesso preliminare al conto, l'intermediario dichiara che per tale accesso - avvenuto tramite un solo fattore di autenticazione valido - varrebbe l'esenzione prevista dall'art. 10 del Regolamento delegato EBA 2018/389, per le attività di consultazione delle informazioni sui conti.
La norma invocata prevede che "*I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, fatto salvo il rispetto dei requisiti di cui all'articolo 2, se l'utente dei servizi di pagamento accede direttamente al suo conto di pagamento online, a condizione che l'accesso sia limitato a uno dei seguenti elementi online senza che siano divulgati dati sensibili relativi ai pagamenti: a) il saldo di uno o più conti di pagamento designati; b) le operazioni di pagamento eseguite negli ultimi 90 giorni attraverso uno o più conti di pagamento designati. 2. In deroga al paragrafo 1, i prestatori di servizi di pagamento non sono esenti dall'applicazione dell'autenticazione forte del cliente se una delle seguenti condizioni è soddisfatta: a) l'utente del servizio di pagamento accede online alle informazioni di cui al paragrafo 1 per la prima volta; b) sono trascorsi più di 180 giorni dall'ultima volta che l'utente del servizio di pagamento ha avuto accesso online alle informazioni di cui al paragrafo 1 ed è stata applicata l'autenticazione forte del cliente*".
Ebbene, ammesso e non concesso che l'attività di visualizzazione del PIN possa astrattamente rientrare nelle attività meramente informative per le quali è prevista l'esenzione, (al contrario, per le operazioni dispositive l'orientamento di questo Collegio è nel senso di negare l'applicabilità della deroga: cfr. Collegio Milano, decisione n. 10636/2024; decisione n. 8155/2024), vi è che la resistente nulla deduca a proposito dell'ultima eventuale applicazione della SCA, sì che il Collegio non può verificare se

questa si è svolta nei 180 giorni precedenti richiesti dall'art. 10 del regolamento citato per l'operare dell'esenzione, né se si è svolta nel rispetto del doppio fattore.
Non si può dunque reputare provata la SCA per la fase di accesso al conto.

In linea con l'orientamento consolidato dell'Arbitro deve ritenersi che il difetto anche parziale della prova di autenticazione è risolutivo e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova di colpa grave dell'utente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 9.900,00.
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