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) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) DELL'ANNA MISURALE

Seduta del 01/04/2025

FATTO

Con ricorso del 4/1/2025, la cliente espone quanto segue:

- in data 24/06/2024 subiva una truffa telefonica;
- riceveva una chiamata da un numero che, secondo una ricerca effettuata su internet, era riconducibile all'intermediario;
- l'interlocutore, qualificatosi come sedicente operatore dell'intermediario, la avvertiva che vi erano alcuni pagamenti in uscita dal suo c/c e le chiedeva di comunicargli i codici ricevuti tramite SMS per bloccare detti pagamenti;
- riceveva svariati SMS tramite il canale abitualmente utilizzato dall'intermediario;
- comunicava telefonicamente i codici ricevuti al sedicente operatore;
- riceveva vere notifiche tramite l'APP dell'intermediario relative ai tentativi di pagamento;
- conclusa la telefonata, contattava l'intermediario al numero del servizio clienti;
- il servizio clienti le riferiva che non erano stati loro a contattarla, che sul suo c/c risultava un bonifico di € 450,00 e che non aveva più accesso al suo *home banking*;
- si avvedeva di essere stata vittima di una truffa;
- presentava denuncia presso le Autorità in data 24/06/2024;
- presentava reclamo all'intermediario in data 18/07/2024, che veniva riscontrato negativamente.

Chiede, pertanto, che le siano restituite le somme indebitamente sottratte.

L'intermediario, riportato il fatto, afferma quanto segue:

- la cliente è titolare di un c/c avente IBAN IT*009, aperto in data 11/04/2023 e di una carta di debito associata;
- l'operazione è stata correttamente contabilizzata, registrata e autenticata in quanto realizzata con il corretto inserimento delle credenziali;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici;
- quanto all'accesso all'area riservata si invoca l'esenzione dalla SCA ex art. 10 Regolamento delegato UE n. 2018/389;
- l'intermediario adotta un sistema di autenticazione forte nel pieno rispetto delle previsioni normative;
- essendo tuttavia consapevole dei differenti orientamenti dei Collegi territoriali in tema di esenzione dalla SCA, l'intermediario chiede la rimessione della questione al Collegio di Coordinamento;
- la cliente è stata vittima di *vishing* in quanto il numero da cui ha ricevuto la telefonata truffaldina non è riconducibile all'intermediario;
- sussiste la colpa grave della cliente in quanto ha dato seguito alle richieste del sedicente operatore dell'intermediario, comunicando i codici OTP ricevuti tramite SMS;
- pertanto, la truffa non è particolarmente sofisticata;
- mette a disposizione dei propri clienti numerose informative circa i possibili rischi di truffa informatica sia sul proprio sito web sia tramite apposite informative inviate alla cliente tramite APP ed e-mail;
- il servizio di SMS-alert è messo a disposizione dei clienti, salvo il loro espresso rifiuto;
- inoltre invia una notifica in APP, nella sezione "I miei messaggi", laddove contatti telefonicamente un proprio cliente così da assicurare la genuina provenienza della telefonata;
- trattandosi di messaggi interni all'APP, essi non possono essere colpiti da SMS *spoofing* e pertanto si tratta di un canale di comunicazione totalmente sicuro per i clienti;
- alla luce di quanto sopra, la cliente avrebbe potuto dubitare circa la provenienza della telefonata truffaldina, adoperando una media diligenza;
- non avrebbe mai potuto impedire l'esecuzione dell'operazione disconosciuta;
- la cliente ha violato con colpa grave l'art. 7 D. Lgs. 11/2010 e l'art. 43 dell'Accordo Quadro per la prestazione dei servizi bancari e di pagamento.

Conclude chiedendo il rigetto del ricorso.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di una operazione di € 450,00 eseguita il 24 giugno 2024, alle ore 11:51. È in atti la denuncia presentata dalla cliente lo stesso giorno.

Viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate. In proposito, va innanzi tutto rilevato che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, n. 11. In particolare, le fonti normative applicabili alla fattispecie sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10

bis del D. Lgs. 11/2010, nelle 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 (v. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico è richiesta l'autenticazione forte (SCA) 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; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Al riguardo, giova precisare che l'art. 10 del D.lgs. n. 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.

Ciò premesso, per quanto attiene al primo profilo sopra individuato, l'intermediario non ha fornito prova della corretta autenticazione forte.

Con riferimento agli accessi all'area riservata, prodromici al reset della password e all'esecuzione dell'operazione contestata, l'intermediario afferma di avvalersi dell'art. 10 del Reg. delegato (UE) 2018/389 che autorizza i PSP a non applicare l'autenticazione forte qualora non siano trascorsi 180 giorni dall'ultima volta che il cliente ha avuto accesso con doppio fattore. Dà dunque prova che la cliente ha fatto accesso all'area con autenticazione forte mediante l'inserimento di username e password + codice OTP ricevuto sul numero di cellulare associato al suo conto nei precedenti 180 giorni.

L'art. 10 del Reg. delegato EBA 2018/389 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, nel caso di specie l'attività che l'accesso all'App ha reso possibile non è attività meramente informativa ma dispositiva e per tale tipo di operazioni l'orientamento di questo Collegio è nel senso di negare l'applicabilità della deroga (v. Collegio Milano, decisione, n. 10636/2024, decisione n. 8155/2024 e decisione n. 7574/2024). Sul punto, il Collegio di Milano ha reputato che la norma invocata limita l'esenzione dalla SCA ai soli accessi di tipo meramente informativo – sì che non possa trovare applicazione

laddove, in concreto, l'accesso sia di tipo dispositivo, in quanto prodromico all'esecuzione delle operazioni di pagamento.
Anche altri Collegi hanno ritenuto che l'accesso al conto "*di natura non meramente informativa, perché seguito dalla disposizione di un bonifico, non risulta conforme ai requisiti normativamente previsti*". In questo senso, Collegio di Bologna, decisione n. 11652/24 e decisione n. 9591/24; nonché Collegio di Bari, decisione n. 6380/2024.
Il Collegio, dunque, reputa che nel caso di specie gli accessi propedeutici alla transazione truffaldina non risultano assistiti da SCA.
Del pari, non può considerarsi esaustiva la prova della SCA con riferimento alla fase di esecuzione del pagamento.
Per detta fase, infatti, l'intermediario, provato il fattore di possesso attraverso la OTP, individua il secondo fattore di autenticazione nel codice CVV dinamico, che qualifica come elemento di "conoscenza".
Per opinione comune dei Collegi, tuttavia, l'autenticazione mediante CVV dinamico deve qualificarsi come elemento di possesso (in tal senso, Collegio di Bari, decisione n. 9345 del 27 settembre 2023; Collegio di Roma, decisioni n. 2840 del 22 marzo 2023 e n. 10679 del 6 novembre 2023; da ultimo, Collegio di Milano, decisione n. 8153 del 13 luglio 2024).
Nella stessa direzione si pongono le indicazioni fornite dall'EBA nell'Opinion del 21 giugno 2019, secondo le quali il CVV dinamico deve qualificarsi come elemento di possesso. Come noto, un doppio fattore di possesso non risulterebbe conforme alla SCA in quanto, in base alla stessa citata Opinion dell'EBA, l'autenticazione forte presuppone il ricorso a due fattori di autenticazione appartenenti a categorie diverse.
In linea con quanto statuito da questo stesso Collegio in presenza di allegazioni analoghe deve, pertanto, reputarsi non provata la SCA (Collegio di Milano, decisione n. 3554 del 20 marzo 2024; Collegio di Milano, decisione n. 8153 del 13 luglio 2024; cfr. inoltre, sempre per un caso riguardante l'intermediario resistente in cui non è stata ritenuta provata la SCA in presenza di CVV dinamico, Collegio di Torino, decisione n. 7207 del 19/06/2024).
In mancanza di prova della SCA il ricorso deve essere accolto integralmente, posto 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 e in linea con la giurisprudenza costante di questo Arbitro, 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 € 450,00.
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