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 20/12/2024, la cliente espone quanto segue:

- alle ore 15:00 del 18/10/2024 riceveva una chiamata da un sedicente operatore antifrode dell'intermediario;
- con la chiamata le veniva riferito che erano state effettuate delle presunte operazioni fraudolente dal suo conto corrente. Il sedicente operatore le chiedeva di condividere lo schermo tramite chiamata su APP di messaggistica e la invitava a scaricare un'applicazione per poter effettuare dei controlli;
- a questo punto provvedeva a scaricare l'applicazione sul proprio telefono e notava che il presunto operatore antifrode riusciva ad interagire con il suo dispositivo a distanza;
- mentre il sedicente operatore, che restava per tutto il tempo al telefono con lei, effettuava le operazioni sul telefono, notava che dall'applicazione risultavano dei bonifici. Alle sue domande riguardo tali operazioni il sedicente operatore rispondeva che era un modo per mettere il suo denaro al sicuro;
- insospettita, metteva in attesa la chiamata su APP di messaggistica con il sedicente operatore e contattava direttamente il *call center* dell'intermediario. Un

operatore di quest'ultimo riferiva che l'intermediario non aveva parte in ciò che stava accadendo e le comunicava un saldo del suo conto che non risultava congruo con la cifra che ricordava;
- decideva quindi di bloccare immediatamente il numero con cui era ancora in chiamata sull'APP di messaggistica e spegneva il telefono;
- procedeva a bloccare il conto e a presentare denuncia presso le Autorità;
- verificava quindi che era stato effettuato in data 18/10/2024 un bonifico di € 2.980,00 con causale "*Addebito per acquisto con carta in esercizi comm. *352 T**";
- presentava reclamo all'intermediario in data 20/11/2024, che veniva riscontrato negativamente.

Chiede, pertanto, la restituzione dell'importo di € 2.980,00.

L'intermediario, riportato il fatto, afferma quanto segue:
- il ricorso è irricevibile in quanto l'operazione disconosciuta è stata correttamente autorizzata mediante l'utilizzo delle credenziali statiche e dinamiche in possesso della cliente stessa con autenticazione forte a due fattori (*Strong Customer Authentication*) e registrate e contabilizzate senza alcun malfunzionamento;
- la cliente è stata vittima di *vishing*;
- sussiste la colpa grave della cliente in quanto la stessa ammette di aver condiviso lo schermo del proprio *smartphone* e di aver scaricato una applicazione su richiesta di un sedicente operatore al telefono, il quale, pertanto, riusciva ad interagire con il suo dispositivo anche a distanza. Durante tale condivisione dello schermo, veniva eseguito il pagamento *online* contestato, mediante la collaborazione della cliente, la quale convalidava le operazioni attraverso il riconoscimento biometrico e la conferma con *token*. Dalla schermata allegata al ricorso relativa alla lista chiamate, si evince che il numero che ha contattato la cliente veniva individuato come *spam*: nonostante lo *smartphone* della cliente avesse individuato una anomalia, la cliente ha dato seguito alle assurde richieste del sedicente operatore al telefono.

L'intermediario chiede, dunque, il rigetto del ricorso.

Segue lo scambio di repliche e controrepliche con le quali le parti ribadiscono le proprie difese.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di una operazione di *e-commerce* eseguita tramite carta di debito in data 18/10/2024, alle ore 15:23 di € 2.980,00.

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 alla fase di accesso all'APP/home banking, l'intermediario afferma di avvalersi dell'art. 10 del Reg. delegato (UE) 2018/389 che autorizza i PSP a non applicare l'autenticazione forte del cliente qualora non siano trascorsi 180 giorni dall'ultima volta che il cliente ha avuto accesso con doppio fattore. Dà dunque prova che in data 01/07/2024 la cliente ha fatto accesso all'App con autenticazione forte mediante il riconoscimento biometrico e una OTP ricevuta sul numero di cellulare associato al suo conto. Sulla base delle evidenze prodotte risulta che i fattori di autenticazione in tale occasione di login in data 01/07/2024 fossero: riconoscimento biometrico (*Tipo de firma – 123*); OTP inviato al numero riportato dalla cliente in denuncia.

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 conferma con Token, 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 € 2.980,00.
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