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 dell'8 gennaio 2025, il cliente espone quanto segue:

- è titolare del c/c avente IBAN IT*129 e di una carta associata n. *561;
- in data 06/11/2024 riceveva un SMS apparentemente proveniente dall'intermediario, con cui veniva informato circa un accesso sospetto al suo c/c;
- contattava il numero indicato nell'SMS, credendo che appartenesse all'intermediario convenuto;
- l'interlocutore disponeva di informazioni dettagliate sulle transazioni del suo c/c, informazioni accessibili solo tramite l'area riservata;
- detto interlocutore gli chiedeva di comunicare i codici OTP ricevuti tramite SMS e il cliente collaborava;
- successivamente si avvedeva di un pagamento non autorizzato per € 1.410,00;
- è stato vittima di una frode sofisticata;
- presentava denuncia presso le Autorità in data 22/11/2024;
- presentava reclamo all'intermediario in data 26/11/2024, che veniva riscontrato negativamente.

Chiede, pertanto, il rimborso dell'importo di € 1.410,00 e che siano esaminate eventuali responsabilità riguardo alla compromissione della sicurezza dei dati personali.

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

- l'operazione disconosciuta 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;
- il cliente è stato vittima di SMS *spoofing* e *vishing*;
- sussiste la colpa grave del cliente in quanto, ricevuto l'SMS, ha chiamato un numero non riconducibile all'intermediario e ha comunicato all'interlocutore i codici OTP ricevuti tramite SMS;
- il cliente avrebbe potuto rendersi facilmente conto che il numero indicato nell'SMS non apparteneva all'intermediario, effettuando una semplice ricerca su internet;
- la truffa non può quindi considerarsi particolarmente sofisticata;
- il truffatore conosceva i dati personali del cliente perché quest'ultimo li ha probabilmente comunicati;
- informa la propria clientela circa i possibili rischi di truffe informatiche, inviando informative tramite e-mail e APP;
- il 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.

Chiede, quindi, il rigetto del ricorso.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di un pagamento con carta eseguito in data 6/11/2024, alle ore 13:48, per € 1.410,00.
È in atti la denuncia presentata dal cliente il 2211/2024.
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 (c.d. PSD 2) in vigore dal 13/01/2018. Segnatamente, la *Strong Customer Authentication* (c.d. SCA) è disciplinata dagli artt. 97 e 98 della PSD 2, dall'art. 10-*bis* del d.lgs. n. 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.
Come stabilito dal Collegio di Coordinamento con decisione n. 22745 del 10 ottobre 2019, l'onere probatorio riguardante l'autenticazione forte e la condotta gravemente colposa del cliente grava sull'intermediario.

Per quanto attiene all'autenticazione forte, l'intermediario afferma che le operazioni contestate sono state correttamente contabilizzate, registrate e autenticate.
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 Reg. 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 accesso prodromica a quella di esecuzione dell'operazione 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: v. Collegio Milano, decisione, n. 10636/2024; decisione n. 8155/2024), vi è che il 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. Ne segue la carenza di SCA per quanto attiene alla fase di accesso all'area riservata.
Del pari, non può considerarsi esaustiva la prova della SCA con riferimento alla fase di esecuzione dei pagamenti. 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 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 linea con l'orientamento consolidato dell'Arbitro deve ritenersi che in mancanza di prova della SCA il ricorso debba 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, un *prius* logico rispetto alla prova di colpa grave dell'utente.
Il cliente articola la domanda chiedendo oltre al rimborso delle somme, che siano esaminate "eventuali responsabilità" dell'intermediario riguardo alla compromissione dei suoi dati personali e "un'indagine più approfondita" sulle modalità con cui i truffatori sono stati in grado di ottenere informazioni al fine di prevenire casi simili. Si tratta, all'evidenza, di domande, peraltro non circostanziate, che esulano dalla competenza di questo Arbitro in quanto meramente consulenziali e che dunque devono considerarsi inammissibili (sul punto cfr. Collegio Napoli, decisione n. 352/2011; nonché Collegio Milano, decisioni nn. 1897/2014 e 4404/2015).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.410,00; dichiara il ricorso inammissibile nel resto.
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