COLLEGIO DI MILANO

composto dai signori:

(MI) ACHILLE	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERSANO

Seduta del 31/07/2023

FATTO

Nella presente controversia, la parte ricorrente afferma quanto segue:

- di aver ricevuto in data 06/04/2022 un SMS apparentemente riconducibile all'intermediario, che lo informava dell'avvenuto blocco dell'utenza per un non meglio precisato "difetto di verifica della sicurezza web" e della necessità di effettuare una procedura cui rimandava apposito link;
- che tale SMS si inseriva cronologicamente nella sequenza delle comunicazioni ufficiali dell'intermediario;
- di essere, quindi, stato indirizzato ad una pagina web all'interno della quale inseriva le proprie credenziali di accesso all'home banking;
- di aver ricevuto, poco dopo, una chiamata da un sedicente operatore dell'ufficio della banca, che riportava il numero ufficiale di assistenza della resistente e che lo invitava a disinstallare e reinstallare dal proprio smartphone l'app dell'intermediario;
- che, dopo aver seguito le istruzioni del presunto operatore, quest'ultimo lo informava che sarebbe stato ricontattato il giorno seguente per ricevere conferma della buona riuscita dell'operazione;
- il giorno successivo, non ricevendo alcuna chiamata, procedeva a chiamare il servizio clienti dell'intermediario; in quell'occasione apprendeva che: 1) non risultava alcun problema di operatività legato al conto corrente o all'app, 2) la banca non aveva inviato alcun messaggio o effettuato alcuna chiamata nella data

interessata 3) era stato disposto dal suo conto un bonifico per € 29.997,00 a favore di terzi;
- in data 08/04/2022 presentava dunque denuncia alle forze dell'ordine e, in seguito, si recava in filiale per ottenere informazioni circa l'accaduto; in quell'occasione riceveva da un addetto allo sportello indicazione di formattare il cellulare per evitare ulteriori attività fraudolente, pregiudicando così la possibilità di versare in atti gli SMS ricevuti in quei giorni e il registro delle chiamate;
- la giurisprudenza della S.C. ha evidenziato come lo standard di diligenza richiesto all'istituto bancario sia estremamente elevato e che la banca, conseguentemente, abbia il dovere di adoperarsi con ogni mezzo necessario al fine di evitare il verificarsi di eventi pregiudizievoli a danno della propria clientela;
- la resistente è stata negligente in quanto non ha adottato sistemi di sicurezza e di controllo idonei, e per non aver rispettato lo schema della c.d. autenticazione forte "a due fattori", non avendo provveduto ad inoltrare alcun messaggio contenente l'OTP necessario ad autorizzare le operazioni dispositive;
- che la banca avrebbe dovuto attivarsi per bloccare l'operazione dal momento che il ricorrente e la moglie – cointestataria del conto corrente da cui è stato disposto il bonifico disconosciuto – prima di allora, non avevano mai disposto bonifici online e mai, in ogni caso, bonifici per importi così ingenti;
- tale operazione doveva essere intercettata come "operazione sospetta" e, secondo un canone di buona fede e correttezza da osservarsi nell'esecuzione del mandato conferitole, la Banca avrebbe dovuto avvertire tempestivamente il cliente dell'operazione fraudolenta.

Il ricorrente chiede, dunque, all'Arbitro, che venga accertato il proprio diritto ad ottenere il rimborso dell'importo di € 29.997,00, somma che ritiene essergli stata fraudolentemente sottratta.

Nelle proprie controdeduzioni, l'intermediario domanda il rigetto del ricorso, affermando quanto segue:

- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto sono avvenute con il corretto inserimento delle credenziali;
- nello specifico, in data 06/04/2022, il cliente ha ricevuto via SMS l'OTP necessario ai fini dell'attivazione del Mobile Token su nuovo dispositivo;
- il cliente ha ammesso in denuncia di aver cliccato sul link contenuto nell'sms "civetta" e di aver seguito le indicazioni fornite dal truffatore via filo circa la disinstallazione e reinstallazione dell'app;
- sussiste dunque la colpa grave del cliente nella custodia delle credenziali, in quanto non avrebbe dovuto comunicare a terzi i codici strettamente personali ricevuti, né inserirli in alcuna pagina web;
- controparte non ha in ogni caso versato in atti alcuna evidenza degli sms e delle chiamate fraudolente ricevute;
- ha da tempo attivato una campagna informativa antifrode a beneficio della clientela, non solo online, ma anche tramite canali fisici;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.

Successivamente, in sede repliche, il cliente domanda, in via principale, di porre a carico dell'intermediario il rimborso della somma sottrattagli pari ad € 29.997,00; in via subordinata, la condanna dell'intermediario ad un indennizzo per il danno patito, da determinarsi secondo equità, precisando che:

- la mancata produzione degli SMS e del registro delle chiamate è da ricondursi esclusivamente alle indicazioni fornite dall'addetto di Filiale che ha suggerito al cliente di formattare il dispositivo mobile;
- la banca non ha osservato una condotta improntata al canone di diligenza richiesto ad un istituto soggetto alla normativa speciale bancaria;
- come affermato dalla S.C., la banca avrebbe dovuto adoperarsi dinanzi al carattere anomalo dell'operazione contestata – inedito per tipologia, beneficiario e importo – attivando i doveri di protezioni sussistenti nei confronti della clientela;
- la banca avrebbe dovuto adoperarsi per sospendere o bloccare la disposizione in parola, senza che ciò potesse considerarsi un'indebita limitazione dell'autonomia negoziale del correntista;
- è stato indotto a ritenere genuino il contatto telefonico della banca, dal momento che la chiamata veniva ricevuta dal numero ufficiale di assistenza dell'istituto e che tale circostanza, unitamente ai messaggi inseriti in coda alla chat contenenti i messaggi genuini, dimostra che il sistema adottato dalla banca per le comunicazioni non risponde a idonei requisiti di sicurezza.

L'intermediario, per contro, in sede di controrepliche, ribadisce tutto quanto già eccepito in sede di controdeduzioni, con specifico riguardo:

- alla corretta autenticazione, registrazione e contabilizzazione dell'operazione;
- alla condotta gravemente colposa del cliente che ha ammesso di aver seguito le indicazioni del finto operatore e di aver installato l'app non ufficiale della banca;
- al mancato assolvimento dell'onere probatorio gravante sul ricorrente per la mancata produzione del messaggio civetta e del registro chiamate;

In relazione alla domanda di riconoscimento di un indennizzo stabilito in via equitativa per il danno patito, rileva che essa deve ritenersi inaccoglibile per difetto di prova dell'*an* e del *quantum debeatur*.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto la contestazione di un'operazione bancaria di importo complessivo pari ad € 29.997,00 (l'importo è comprensivo di € 1,00 di commissione, di cui pure viene richiesto il rimborso), effettuata in data 06/04/2022 alle ore 16.50.

A detta data era vigente il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D. Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU.

In forza di tale disciplina, in caso di contestazione delle operazioni, grava sull'intermediario l'onere di provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire evidenza di aver applicato un c.d. "Sistema di autenticazione forte" (strong customer authentication o SCA), posto che ai sensi del comma 2-bis dell'art. 12 d. lgs. n. 11/2010, come inserito dal d. lgs. n. 218/2017, *"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 beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente"*. L'intermediario, inoltre, è anche tenuto a provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento (art. 12, co.

2-ter e s., d. lgs. n. 11/2010).

L'intermediario afferma che le operazioni sono state correttamente contabilizzate, registrate e autenticate.

Con riferimento alla strong customer authentication (c.d. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'art. 10-*bis* del D. Lgs. 10/2011, 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, l'autenticazione forte (SCA) è richiesta sia nella fase di (i) accesso al conto/ enrollment dell'app/registrazione della carta sul wallet, sia nella fase di (ii) esecuzione delle singole operazioni. 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.

Con riferimento alla prova dell'autenticazione forte nella fase di accesso all'app, secondo la ricostruzione dell'intermediario alle ore 16:50 del 6/04/2022 sarebbe stato effettuato un accesso all'app tramite PIN e OTP.

Nei log prodotti è riportato l'OTP generato ai fini dell'accesso. Quanto invece all'altro fattore di autenticazione (PIN) nei LOG non è presente conferma del suo inserimento, il cui utilizzo risulta riportato solo nella descrizione attività utente.

Dalle evidenziate lacune probatorie quanto all'autenticazione, alla corretta registrazione e alla contabilizzazione delle operazioni mediante un c.d. "Sistema di autenticazione forte" consegue che, ad avviso del Collegio, l'intermediario resistente non ha provato di aver adottato gli standard di sicurezza corrispondenti alla disciplina oggi applicabile come sopra individuata, dovendosi altresì ricordare che secondo il disposto dell'art. 10, co. 1, d.lgs. n. 11/2010 *"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".*

A tale riguardo e in siffatto contesto, a differenza di quanto accade per la colpa grave dove si deve ammettere la possibilità di ricorrere alle presunzioni, per la SCA la prova non può essere indiziaria o indiretta, ma deve avere ad oggetto specificamente i singoli fattori di autenticazione, dovendo il prestatore di servizi di pagamento offrire puntuale evidenza di quali siano stati quelli in concreto ed effettivamente utilizzati, nonché del completo processo attraverso cui sono stati utilizzati (in questo senso, vd. ABF-Coll.- Milano n. 6881 del 5 luglio 2023 e n. 6933 del 6 luglio 2023).

Ciò premesso, rispetto alla mancanza anche parziale della prova di autenticazione, i Collegi sono unanimi nel ritenere che in tali casi il ricorso venga accolto integralmente, posto che il difetto di tale prova 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.

Questo Collegio ritiene che la documentazione allegata dalla parte resistente non sia esaustiva circa la prova dell'avvenuta autenticazione delle operazioni contestate; da ciò

consegue che ogni ulteriore valutazione in merito alla sussistenza o meno della colpa grave in capo al ricorrente è del tutto irrilevante e la domanda restitutoria deve essere accolta.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 29.997,00.

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
DAVIDE ACHILLE