COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) PEDERZOLI	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore DANIELE PERSANO

Seduta del 25/06/2024

FATTO

Nel presente procedimento, la parte ricorrente afferma quanto segue:

- in data 07.07.2023 acquistava presso la propria filiale una nuova carta prepagata (emessa da altro intermediario) n. *** 1468 collegata al proprio conto corrente personale poiché la precedente carta prepagata era in scadenza;
- in data 12.07.2023 riceveva un primo SMS apparentemente proveniente dall'intermediario emittente con il quale veniva informata del blocco della carta per la mancata verifica di alcune procedure di sicurezza e, poi, un secondo sms che le preannunciava una chiamata da un presunto operatore dell'intermediario;
- in data 14.07.2023 riceveva una chiamata apparentemente proveniente dal numero ufficiale dell'intermediario, durante la quale un sedicente operatore la invitava a seguire le proprie indicazioni per risolvere la questione;
- verificava l'autenticità del mittente provando a richiamare il numero, a cui rispondeva effettivamente la segreteria telefonica dell'intermediario convenuto;
- non ha mai comunicato né digitato alcuna password durante i contatti telefonici con il truffatore;
- in data 17.07.2023 riscontrava che dal proprio corrente personale era stata indebitamente sottratta una somma di denaro pari ad € 3.200,00 mediante un bonifico bancario non autorizzato indirizzato ad un terzo sconosciuto;

- ha presentato denuncia presso le Autorità competenti;
- ha presentato reclamo, riscontrato negativamente dall'intermediario.

La ricorrente chiede, dunque, all'Arbitro, che venga accertato il proprio diritto ad ottenere il rimborso dell'importo che ritiene esserle stato fraudolentemente sottratto pari ad € 3.200,00, oltre ad € 2,00 per il costo del bonifico effettuato ed € 20,00 per la presentazione del ricorso.
Nelle proprie controdeduzioni, l'intermediario domanda, in via principale, il rigetto del ricorso, mentre, in via subordinata, laddove dovesse ravvisarsi una qualche responsabilità della Banca, chiede che venga accertato un concorso di colpa ai sensi dell'art. 1227 c.c. In particolare, eccepisce quanto segue:

- la cliente è titolare di un c/c acceso presso una filiale dell'intermediario dove sono attivi i servizi di banca telematica **;
- al momento dell'attivazione del servizio di home banking, la cliente ha fornito i suoi contatti associati alla sua utenza, dalla stessa mai modificati;
- sempre in occasione dei servizi di banca telematica, sono stati forniti il codice utente e la password noti solo alla cliente;
- dalle verifiche svolte è emerso che l'operazione disconosciuta è stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali e preceduta dalla disinstallazione dell'APP sul dispositivo della cliente e dalla installazione dell'APP sul dispositivo dei frodatori;
- inoltre, può essere installata una sola APP su un unico dispositivo;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici;
- deve presumersi la colpa grave della cliente, la quale ha tenuto un comportamento attivo e collaborativo per l'esecuzione della truffa; nel caso in specie, infatti, ha (i) cliccato su un link contenuto in un SMS apparentemente riconducibile ad altro intermediario; (ii) verosimilmente comunicato la password per installare la APP sul device dei frodatori; (iii) intrattenuto una telefonata con un presunto operatore bancario e seguito pedissequamente le istruzioni impartite;
- la Corte di Cassazione, con ordinanza n. 7214 del 13.03.2023, ha chiarito che l'intermediario non è tenuto al risarcimento in presenza di una condotta gravemente negligente del cliente;
- l'intermediario ha attivato apposite campagne informative antifrode, volte a sensibilizzare la clientela rispetto alle forme di truffa più diffuse.

Successivamente la cliente, in sede di repliche, ribadisce quanto affermato in sede di ricorso ed insiste per l'accoglimento.
L'intermediario, per contro, con le controrepliche, riportandosi alle conclusioni in atti, insiste nelle medesime argomentazioni difensive già svolte in sede di controdeduzioni.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto la contestazione di un'operazione di bonifico tramite home banking non autorizzata dell'importo complessivo di € 3.200,00, effettuata in data 14.07.2023 alle ore 15:17.
Alla data dell'operazione 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 l'operazione è stata correttamente contabilizzata, registrata e autenticata.
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.
Quanto alla fase di enrollement, l'intermediario rileva che alle ore 14:38 del 14.07.2023 è stata attivata una nuova licenza "*appmobile*", presumibilmente dal terzo truffatore sul proprio dispositivo, il quale, per attivare la nuova licenza, ha dovuto necessariamente inserire correttamente "Utenza + Password + OTP ricevuto via email + OTP ricevuto via SMS sul cellulare certificato dalla cliente in fase di contrattualizzazione". Precisa che l'app può essere installata su un unico dispositivo mobile per volta, sicché l'attivazione dell'app/licenza smart OTP sul nuovo dispositivo è stata preceduta dalla disinstallazione della app sul device della cliente.
L'intermediario ha prodotto le evidenze informatiche (corredate da legenda esplicativa) relative a tale fase dalle quali non è possibile evincere alcun inserimento della password (elemento di conoscenza), necessario sulla base della procedura descritta dall'intermediario; l'inserimento di utenza + password, quale elemento necessario dell'autenticazione, viene menzionato solo nella legenda esplicativa / esposizione descrittiva dei log.
L'intermediario rileva che alle ore 15:13, a seguito di precedenti *login* effettuati senza disporre alcuna transazione, è stato eseguito un accesso dal nuovo dispositivo inserendo correttamente il codice utente e la password personali della cliente e il PIN dispositivo impostato.
Quanto all'accesso, la legenda prodotta specifica che, ai fini del login, l'applicazione richiede l'inserimento di Utenza + Password + PIN; e che la dicitura ESITO = 000 conferma l'inserimento di tutti i parametri di sicurezza previsti.
Dall'esame dei log, si rileva che non vi è evidenza dell'inserimento di Utenza + Password + PIN che secondo l'intermediario sarebbero richiesti per l'accesso; è la legenda esplicativa a indicare che l'applicazione richiede ad ogni accesso UTENZA + PASSWORD + PIN DISPOSITIVO.

Quanto all'operazione disconosciuta, l'intermediario rileva che il bonifico risulta eseguito alle ore 15:17, e specifica che per l'autorizzazione dell'operazione di pagamento riepilogata tramite notifica *push* è stato necessario inserire il codice utente e la password personale e il PIN dispositivo.
Da quanto prodotto, non vi è evidenza dell'inserimento del PIN ai fini dell'autorizzazione del bonifico.
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 € 3.202,00.
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
FLAVIO LAPERTOSA