COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) BARILLA'	Membro designato dalla Banca d'Italia
(MI) MANENTE	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) MANENTE

Seduta del 12/07/2022

FATTO

Con ricorso presentato nella data sopra indicata parte attrice, titolare presso l'intermediario di un conto corrente a cui è associata la carta bancomat, ha esposto quanto segue:

- in data 25/06/2021 aveva ricevuto sul suo cellulare una notifica di pagamento di € 100,00, mai autorizzato, a favore di una fondazione, seguita da una chiamata proveniente da un'utenza privata **411;
- nella telefonata un sedicente operatore dell'intermediario la informava di alcuni movimenti eseguiti con l'utilizzo del bancomat e le forniva le istruzioni per procedere allo storno dell'importo di cui sopra e al blocco delle operazioni sospette;
- secondo le istruzioni impartite dal presunto operatore, la ricorrente accedeva al proprio *home banking* dalla App installata sul suo cellulare; aumentava i massimali operativi della carta bancomat; cliccava su una impostazione presente in App; autorizzava infine l'operazione di pagamento di € 2.900,00 a favore della carta R*;
- successivamente si rendeva conto di essere stata vittima di una truffa e procedeva al blocco dello strumento di pagamento e al disconoscimento delle operazioni.

Ciò premesso, ha chiesto al Collegio il rimborso di quanto indebitamente sottrattole a seguito della truffa.

L'intermediario ha trasmesso le proprie controdeduzioni, nelle quali, in via preliminare, ha eccepito l'inammissibilità del ricorso per incompetenza dell'Arbitro/inapplicabilità della legge italiana, allegando che:

- il conto corrente della cliente è radicato presso la casa madre dell'intermediario in Germania;
- la ricorrente ha dichiarato il proprio indirizzo di residenza in Germania e non ha informato l'intermediario di eventuali variazioni;
- il contratto quadro stipulato con la cliente, al quale si applica il diritto tedesco, prevede che eventuali doglianze debbano essere presentate ad un organo stragiudiziale diverso dall'ABF, ovvero alla Banca Federale Tedesca o all'Autorità tedesca di Vigilanza.

Quanto al merito, ha dedotto che:

- la ricorrente è stata vittima di c.d. *vishing*;
- l'operazione di € 2.900,00, avvenuta con il corretto inserimento delle credenziali, è stata correttamente contabilizzata, registrata e autenticata
- l'operazione di € 100,00 costituisce, in realtà, un'operazione di pre-autorizzazione, già stornata dall'esercente commerciale.

Conseguentemente, ha chiesto al Collegio, in via principale, di dichiarare l'inammissibilità del ricorso; in via subordinata, di respingere il ricorso; in ogni caso, di dichiarare la cessazione della materia del contendere con riguardo all'operazione di € 100,00.

La ricorrente ha presentato replica, nella quale, contestando le difese dell'intermediario, ha affermato che questo non ha dimostrato di aver adottato un sistema di autenticazione forte.

L'intermediario ha, a propria volta, trasmesso controreplica, nella quale, ribadita la regolare autenticazione dell'operazione disconosciuta, ha ripetuto le conclusioni precedentemente formulate.

DIRITTO

La controversia in decisione attiene alla domanda di rimborso di somme indebitamente sottratte a seguito di operazioni *on-line* disconosciute.
Il Collegio deve preliminarmente esaminare l'eccezione di inammissibilità del ricorso per incompetenza dell'Arbitro/inapplicabilità della legge italiana, essendo il rapporto assoggettato alla legge tedesca per le ragioni esposte nella parte in fatto di cui sopra.
L'eccezione è infondata.

Al di là di ogni altra pur possibile considerazione (basti notare, ad esempio, che a sostegno dell'applicabilità della legge italiana depongono il fatto che dagli albi ed elenchi ufficiali della Banca d'Italia risulta che l'intermediario ha una succursale in Italia, con la quale la ricorrente intrattiene il rapporto, e che la corrispondenza precedente alla proposizione del ricorso è a firma tanto della succursale italiana quanto della casa madre tedesca, così come il riscontro al reclamo), è sufficiente rilevare, infatti, che l'intermediario non ha versato in atti il contratto *inter partes* sottoscritto dalla cliente dal quale dovrebbero risultare le clausole (che, tra l'altro, quand'anche non vessatorie la ricorrente avrebbe

comunque dovuto approvare specificamente) sulle quali ha fondato l'eccezione, limitandosi a rinviare in via generale al suo sito web.

Venendo al merito della controversia, le operazioni contestate dal ricorrente rientrano nell'ambito di applicazione della disciplina del D. Lgs. 27.1.2010, n. 11 di recepimento della Direttiva 2007/64/CE sui servizi di pagamento, come modificata dal D. Lgs. 15 dicembre 2017, n. 218 di recepimento della Direttiva 2015/2366 UE, in vigore dal 13/01/2018.

La novellata normativa ha confermato, rafforzandolo, il regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utenti già introdotto dal D. Lgs. n. 11/2010 ante modifica e ripetutamente evidenziato da numerose decisioni dell'ABF, anche del Collegio di Coordinamento (cfr. Decisioni n. 991/2014, n. 5304/2014, n. 3498/2012). Ai fini che interessano la presente decisione vengono in considerazione le seguenti principali disposizioni precettive: *a*) l'art.10, comma primo, stabilisce che, in caso di disconoscimento di un'operazione di pagamento da parte dell'utente, è onere del prestatore di servizi di pagamento provare che essa è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; *b*) con riguardo a quest'ultimo profilo l'art. 8 (fatti salvi gli obblighi posti in capo all'utente dall' art. 7 di cui *infra*) stabilisce una serie di obblighi gravanti sul prestatore dei servizi volti a salvaguardare la sicurezza del sistema, primo fra tutti quello di assicurare l'inaccessibilità ai terzi delle credenziali di sicurezza personalizzate; *c*) in difetto della prova della corretta autenticazione viene meno la possibilità stessa di riferire le operazioni contestate al cliente; *d*) l'art. 10, comma secondo, precisa che, in ogni caso, l'apparente corretta autenticazione non è, di per sé, necessariamente sufficiente a dimostrarne la riconducibilità all'utente che la disconosca, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'art. 7, essendo invece onere del prestatore dei servizi fornire la prova della frode, del dolo o della colpa grave dell'utente; *e*) di seguito, l'art. 12, comma primo, pone a carico del prestatore di servizi di pagamento le perdite derivanti dall'utilizzo dello strumento smarrito, sottratto o utilizzato indebitamente, intervenuto *dopo* la comunicazione di smarrimento o furto prevista dall'art. 7, comma primo, lett. b) ; *f*) l'art. 12, terzo comma, poi, nel prevedere la franchigia di € 50,00 entro la quale l'utente può essere tenuto a sopportare la perdita derivante dalle operazioni compiute *prima* della comunicazione di cui sopra, fa salva l'ipotesi che l'utente «*abbia agito in modo fraudolento o non abbia adempiuto ad uno o più di cui all'art. 7 con dolo o colpa grave*>>, nel qual caso l'intera perdita resta a suo carico; *g*) l'art. 12, comma 2 – *bis* stabilisce inoltre che <<*salvo il caso in cui abbia gito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente*>>, come definita dall'art. 1 lett. q-*bis* ("*un' autenticazione basata sull'uso di due o più elementi classificati nelle categorie della conoscenza* [*qualcosa che solo l'utente conosce*], *del possesso* [*qualcosa che solo l'utente possiede*] *e dell'inerenza* [*qualcosa che caratterizza l'utente*], *che sono indipendenti in quanto la violazione di uno non compromette l'affidabilità degli altri e che è concepita In modo tale da tutelare la riservatezza dei dati di autenticazione*": le relative norme tecniche di regolamentazione sono indicate dal Regolamento delegato UE 2018/389,), necessaria, ai sensi dell'art. 10-*bis*, quando l'utente accede al suo conto di pagamento *on-line*, dispone un'operazione di pagamento elettronico ovvero "*effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*"; *h*) l'art. 7 enuclea gli obblighi gravanti sull'utente abilitato all'utilizzo di uno strumento di

pagamento; in particolare, questi è tenuto ad utilizzare detto strumento nel rispetto delle condizioni contrattuali che ne disciplinano l'emissione e l'uso, i cui termini devono essere obiettivi, non discriminatori e proporzionati (comma primo, lett. a); il comma secondo precisa poi che, *"ai fini di cui al comma 1, lettera a), l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a proteggere le credenziali di sicurezza personalizzate".*

Conclusivamente, quindi, la disciplina in parola applicabile al caso in esame fa discendere un duplice ed alternativo regime di responsabilità per l'utilizzo non autorizzato di strumenti o servizi di pagamento: il primo, per il quale, rispetto alle operazioni poste in essere anteriormente alla tempestiva comunicazione al prestatore dei servizi, l'utente è tenuto a sopportare la perdita derivante dall'utilizzo non autorizzato dello strumento o del servizio di pagamento nei limiti della franchigia di Euro 50,00, rimanendo il resto a carico del prestatore dei servizi; il secondo, che opera nei soli casi in cui l'utente abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'art. 7 con dolo o colpa grave, per il quale l'utente assume invece una responsabilità illimitata e, conseguentemente, sopporta integralmente la perdita.

Passando adesso allo specifico del caso portato in decisione, rileva il Collegio, prima di tutto, che l'operazione di € 100,00 risulta essere già stata riaccreditata sul conto corrente dell'attrice, per cui è venuta meno la materia del contendere *in parte qua*.

Quanto all'operazione di pagamento *on-line* di € 2.900,00 – l'unica di cui resta da discutere – il Collegio osserva che l'intermediario non ha versato in atti la necessaria documentazione completa volta a soddisfare l'onere probatorio prescritto dal sopra citato art. 10, comma primo, D. Lgs cit. e a comprovare l'utilizzo dell'autenticazione forte richiesta dalla legge.

A tale riguardo si ricorda che l'autenticazione forte (SCA) è necessaria 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.

Nel caso di specie l'intermediario ha affermato, in particolare, che l'operazione sarebbe stata autorizzata, tra l'altro, mediante l'invio di un *push* al *device* associato al cliente, ma di esso non vi è in atti alcuna evidenza.

Non essendo, pertanto, stata interamente comprovata la corretta e regolare autenticazione dell'operazione, non è possibile accedere alla successiva valutazione del comportamento dell'utilizzatore ai fini dell'applicazione delle previsioni del successivo art. 12, terzo comma.

Conseguentemente il Collegio deve accogliere la domanda di rimborso dell'operazione disconosciuta di € 2.900,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.900,00.
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