COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERON

Seduta del 20/07/2023

FATTO

Part ricorrente rappresenta al Collegio di essere stata vittima di una truffa di uno *spoofing*, con conseguente sottrazione di € 18.063,00 dal proprio conto corrente aperto presso l'intermediario.
In particolare, è accaduto che in data 29.12.2022, parte ricorrente riceveva un *sms* che l'informava di un'avvenuta limitazione del proprio conto e l'invitava a cliccare un *link* che conduceva ad una piattaforma in cui inserire le credenziali di accesso al sito della banca.
Subito dopo riceveva una chiamata da un numero di telefono fisso corrispondente alla filiale dell'intermediario, con quale un sedicente operatore dell'intermediario l'invitata a resettare la *password* statica di accesso all'applicazione e una volta proceduto in tal senso di inserirla nella piattaforma N** raggiunta tramite il *link* contenuto nel messaggio.
Parte ricorrente veniva ricontattata dal medesimo operatore il giorno seguente e quello ancora successivo al fine di monitorare, a suo dire, il buon andamento dell'operazione; costui prometteva di ricontattarla anche il terzo giorno consecutivo, ma poiché ciò così non avveniva, parte ricorrente chiamava il servizio clienti dell'intermediario e si rendeva conto di aver subito una truffa, realizzata a mezzo di cinque bonifici per complessivi € 18.063,00.
Parte ricorrente formulava pertanto reclamo che veniva però respinto dall'intermediario.

Con specifico riferimento alla truffa parte ricorrente sottolinea di non aver mai ricevuto:

- alcun codice *otp* né via *sms* né via e-mail da poter comunicare ai frodatori, né qualsivoglia altro elemento utile per poter installare l'*app* su altro dispositivo; comunicazioni a mezzo e-mail di intervenuta esecuzione dei bonifici disconosciuti;
- ricevuto notizie sulla richiesta dell'intermediario rivolta alla banca del beneficiario dei bonifici per tentare il recupero delle somme.

Secondo parte ricorrente, l'intermediario è venuto meno all'applicazione dei principi antifrode a tutela dell'utente, delineati dal D.M. 112/2007; infatti dall'apertura del conto corrente alla data del verificarsi della truffa, dato che

- non ha mai effettuato bonifici ricorrenti o prelevato somme di denaro cospicue, limitandosi a farvi accreditare lo stipendio e al prelievo della rata del mutuo;
- le operazioni di bonifico contestate non rientrano nel suo normale comportamento.

Alla luce di quanto sopra parte ricorrente chiede al Collegio di accertare che il sistema di autenticazione non rispetta i requisiti di cui al D.lgs. 11/2010 e che in ogni caso non ha funzionato correttamente essendo stato violato dai frodatori. Chiede pertanto di disporre il rimborso totale delle perdite subite pari a € 18.063,00, oltre al rimborso delle spese di procedura.

L'intermediario controdeduce eccependo anzitutto l'incompetenza *ratione materiae* dell'ABF in quanto il ricorso attiene (anche) ad un'asserita violazione in tema di trattamento dei dati personali che esula dalla competenza dell'Arbitro.

Nel merito, invece, afferma che parte ricorrente è incorsa in colpa grave, dato che la frode non si sarebbe mai perfezionata qualora la stessa avesse evitato di comunicare al terzo frodatore le credenziali personali di accesso all'*home banking* nonché gli *otp* necessari per l'attivazione di una nuova licenza "*smartOTP*". Afferma inoltre

- che le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali.
- che al termine di ogni operazione il sistema della Banca invia all'indirizzo e-mail collegato all'utenza del cliente le relative e-mail di notifica dell'esecuzione delle operazioni, come è avvenuto anche nel caso di specie;
- che a seguito della segnalazione della cliente, l'intermediario ha esperito un tentativo di recall dei bonifici disconosciuti, che non ha tuttavia avuto esito positivo.

In ogni caso fa presente di aver attivato apposite campagne informative anti-frode, volte a sensibilizzare la clientela rispetto a forme di truffa analoghe a quella perpetrata nella specie.

Per tali motivi l'intermediario chiede in via preliminare che il ricorso si dichiarato inammissibile e/o irricevibile in quanto avente ad oggetto anche contestazioni circa la "violazione del trattamento dei dati personali – Privacy" che non rientrano nelle materie di competenza dell'ABF.

In ogni caso chiede che vengano respinte tutte le contestazioni sollevate da parte ricorrente e in via subordinata qualora dovesse ravvisarsi un qualsivoglia responsabilità a suo carico chiede sin d'ora che si tenga conto del comportamento colpevole e imprudente tenuto da parte ricorrente essendo questo rilevante ai fini di un concorso di colpa ai sensi dell'art. 1227 c.c.

Nelle repliche parte ricorrente, richiamati i propri scritti, sostiene di essere stata contatta da un operatore che dichiarava essere un operatore dell'intermediario, di non aver mai ricevuto il secondo codice OTP inviato via *sms*, necessario all'installazione dell'*app* dell'intermediario sul cellulare e che per effettuare le operazioni bancarie come i bonifici è richiesto solo il *pin* dispositivo (mai comunicato ai frodatori) o l'impronta digitale. Precisa, infine, di non aver chiesto l'accertamento della violazione del D.lgs. 11/2010 ragion per cui non si può ravvisare alcun profilo di inammissibilità né parziale né totale del ricorso.
L'intermediario, controreplica affermando quanto segue:

- la cliente non è stata contatta dal terzo frodatore solo attraverso un numero di telefono riconducibile alla banca, bensì, nei giorni successivi, è stata contattata sempre da un diverso numero di telefono, che non è in alcun modo riconducibile alla banca;
- contesta l'invocata applicabilità al caso di specie dei "principi antifrode" delineati dal D.M. 112/2007 in quanto il decreto concerne l'"Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento" e, dunque, attiene ad una fattispecie all'evidenza diversa rispetto alla presente avente ad oggetto bonifici.

DIRITTO

La controversia in esame attiene all'accertamento del diritto di parte ricorrente ad ottenere il rimborso, da parte dell'intermediario resistente, della somma di € 18.063,00, inerente a cinque operazioni di bonifico eseguite dalle ore 17:22 del 29.12.2022 sino alle ore 14:35 del 03.01.2023. In particolare trattasi di bonifici eseguiti in 5 giorni diversi, nell'arco complessivo di 5 giorni.
In via preliminare, il Collegio deve esaminare l'incompetenza *ratione materiae* dell'ABF in quanto il ricorso atterrebbe (anche) ad un'asserita violazione della disciplina in materia di privacy - trattamento dei dati personali, che esula dalla competenza dell'Arbitro.
Il Collegio al riguardo osserva che la cliente, nel ricorso, si limita a rilevare come i sistemi della banca non possano essere considerati sicuri, alla luce del fatto che i frodatori sono riusciti a violarli con facilità. Si tratta tuttavia di una mera considerazione di parte ricorrente riportata a supporto della contestazione relativa al mancato rispetto, da parte della banca, dei requisiti imposti ai PSP dal D.lgs. n. 11/2010. In ogni caso nelle proprie domande parte ricorrente non richiede al Collegio di accertare la violazione, da parte della banca, della disciplina prevista in materia di trattamento dei dati personali.
Alla luce di quanto sopra l'eccezione dell'intermediario è infondata e dev'essere rigettata.
Tanto premesso, si osserva che le operazioni in esame sono disciplinate del D. Lgs. 27.1.2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del relativo Provvedimento attuativo della Banca d'Italia del 5.7.2011. Come è noto, i principi fissati da tale impianto normativo, in materia di strong customer authentication (SCA), fissano due passaggi ineludibili che attengono al piano degli oneri probatori: *a)* è l'intermediario a dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, avendo presente che l'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / *enrollment* dell'applicazione / registrazione della carta sul

wallet, sia nella fase di esecuzione delle singole operazioni; *b)* è sempre l'intermediario a dover 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. In quest'ambito dunque, costante giurisprudenza arbitrale, ritiene che l'eventuale negligenza del cliente possa solo venire in rilievo solo allorquando l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di *alert* (cfr. *ex multis* Collegio di Milano, decisione n. 8262/2020).
Il caso in esame è una fattispecie di *sms spoofing*, misto a ID *caller spoofing*. Tale tipo di truffa è considerato come potenzialmente più decettivo rispetto al comune *phishing* o *vishing*, che si ritiene possano essere contrastato con l'uso di una diligenza minima, in considerazione della loro diffusione e della generalmente scarsa idoneità a trarre in inganno i clienti.
Ciò posto, si impone dunque in prima battuta la verifica sul sistema di autenticazione predisposto dall'intermediario e sul rispetto dei requisiti di cui alla predetta disciplina, avendo egli l'onere di provare *(a)* 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*»; *(b)* che il sistema di autenticazione e l'autorizzazione delle operazioni di pagamento contestate sono conformi alla SCA, che 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, l'intermediario sostiene che le operazioni sono state correttamente contabilizzate, registrate e autenticate e ricostruisce come segue l'operatività fraudolenta:

a) registrazione di un nuovo dispositivo sull'*app*, con attivazione del servizio "*licenza smart OTP*";
b) accesso all'*app* dal nuovo dispositivo;
c) esecuzione delle operazioni disconosciute.

Con riguardo al punto ***a)*** sopra indicato, l'intermediario rappresenta:
- che alle ore 17:13 del 29.12.2022 è stata attivata una nuova licenza "*smartOTP*" presumibilmente dal terzo frodatore sul proprio dispositivo mobile Android;
- che il frodatore, per attivare la nuova licenza *smartOTP*, ha dovuto inserire UTENZA + PASSWORD + OTP ricevuto via e-mail + OTP ricevuto via *sms* sul cellulare della cliente.

Tuttavia, il Collegio osserva che dalla documentazione in atti non è provata l'evidenza dell'inserimento di Utenza + Password. Inoltre:
- quanto all'inserimento del primo codice OTP, l'intermediario allega evidenza nella quale è indicato l'invio all'indirizzo e-mail della cliente l'evidenza, tuttavia, non riporta il testo dell'e-mail con la quale sarebbe stato comunicato il codice OTP;
- quanto all'inserimento del secondo codice OTP, l'intermediario allega evidenza nella quale è indicato l'invio di un "*sms* OTP" al cellulare della cliente alle ore 17:13 del 29.12.2022, ma dall'evidenza sopra riportata non è possibile evincere il contenuto dell'*sms* che dovrebbe contenere il codice OTP.

Con riguardo al punto *b)* sopra indicato, l'intermediario afferma che pochi secondi dopo l'attivazione della nuova licenza "*smartOTP*" i sistemi hanno registrato un accesso all'*home banking* tramite *app* proprio dal medesimo indirizzo IP ****16 che aveva attivato

la nuova licenza. Tale accesso è possibile previo inserimento di Utenza + Password + PIN DISPOSITIVO. Tuttavia, si rileva al riguardo che, dall'esame dei *log*, non vi è evidenza dell'inserimento di Utenza + Password + PIN DISPOSITIVO. Nella legenda è altresì specificato che il *pin* può essere inserito anche mediante credenziali biometriche, ma ad ogni modo non vi è evidenza dell'attivazione di forme di riconoscimento biometrico. Peraltro, analogamente a quanto riportato con riferimento al *login* nell'*app* delle ore 17.13, non risultano prodotte evidenze circa l'inserimento di Utenza + Password + PIN neppure con riferimento ai *login* eseguiti per effettuare i successivi bonifici.
Con riguardo al punto *c)* sopra indicato, l'intermediario afferma che l'esecuzione dei bonifici, è avvenuta tramite *app* con inserimento del *pin* dispositivo, per autorizzare l'operazione che viene riepilogata mediante notifica in *app*. Tuttavia, dall'esame dei *log* si rileva che non vi è evidenza dell'inserimento dei fattori di autenticazione.

In forza dei rilievi sopra evidenziati circa l'assenza di evidenze in merito all'inserimento:

- di Utenza + Password, per l'attivazione della nuova licenza *smartOTP*;
- di Utenza + Password + PIN DISPOSITIVO per l'accesso all'app dal nuovo dispositivo;
- dei fattori di autenticazione per l'autorizzazione delle operazioni contestate,

non risulta raggiunta la prova che le operazioni contestate siano state eseguite a seguito di una corretta "autenticazione forte" (cfr., Collegio di Milano, decisione n. 5716/2023; Collegio Torino, decisioni n. 3653/2023 e n. 16048/2022).
Conseguentemente, anche a prescindere dalla dimostrazione di una condotta gravemente colposa di parte ricorrente (in relazione alla quale incidentalmente il Collegio osserva che l'*sms* civetta era inserito in una *chat*, contenente precedenti messaggi genuini provenienti dall'intermediario, e non presentava errori, mentre la chiamata proveniva da un numero riconducibile all'intermediario), rimangono a carico dell'intermediario le operazioni contestate, non essendo stati da questi assolti gli oneri probatori di cui è gravato con riguardo alla SCA.
Per tali motivi il collegio accoglie integralmente il ricorso.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 18.063,00.
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