## COLLEGIO DI MILANO

composto dai signori:

| | |
|---|---|
| (MI) LAPERTOSA | Presidente |
| (MI) DELL'ANNA MISURALE | Membro designato dalla Banca d'Italia |
| (MI) RIZZO | Membro designato dalla Banca d'Italia |
| (MI) CORNO | Membro di designazione rappresentativa degli intermediari |
| (MI) PERSANO | Membro di designazione rappresentativa dei clienti |

Relatore (MI) PERSANO

Seduta del 12/03/2024

## FATTO

Nel presente procedimento, la parte ricorrente afferma quanto segue:

- è titolare di un conto corrente bancario digitale presso l'intermediario;
- in data 03.01.2023 riceveva sul suo cellulare un sms dall'intermediario, con il quale la si invitava a cliccare un link per accedere al proprio conto corrente tramite *internet banking*, a causa di un asserito accesso anomalo;
- in buona fede, data la provenienza del messaggio, la cliente cliccava sul link e le si apriva una schermata di fatto identica a quella del sito genuino;
- poco dopo riceveva una chiamata telefonica da un interlocutore che si definiva come appartenente ad altro intermediario B (non convenuto), presso il quale la ricorrente possiede un altro conto corrente, informandola della necessità di intervenire su alcune operazioni sospette;
- l'interlocutore la induceva a comunicare i codici contestualmente inviati;
- in seguito, si accorgeva dell'avvenuto addebito sul proprio conto corrente di n. 4 operazioni in uscita da € 2.990,00, € 4.900,00, € 4.990,00 ed € 1.530,00 a favore dell'esercente "B**";

- in data 09.01.2023, dopo essersi avveduta delle operazioni fraudolente, si recava presso la Stazione dei Carabinieri locale per sporgere regolare denuncia;
- in data 31.03.2023 chiedeva il rimborso di quanto sottratto agli intermediari coinvolti, senza ottenere un positivo riscontro;
- l'intermediario convenuto è responsabile ai sensi del D.lgs. 196/2003 e dell'art. 2050 c.c.; non avendo adottato misure al fine di prevenire un illecito accesso ai dati sensibili personali (cfr. decisioni in questo senso dell'ABF e di legittimità, in casi analoghi);
- ricerche eseguite via web confermano che da mesi il sito dell'intermediario è stato oggetto di attacchi informatici che hanno portato a numerosi casi di *vishing*/*phishing* a danno dei clienti.

La ricorrente chiede, dunque, all'Arbitro, che venga accertato, in via principale, il proprio diritto ad ottenere il rimborso dell'importo che ritiene esserle stato fraudolentemente sottratto pari ad € 11.420,00.

In via subordinata, domanda la condanna dell'intermediario al rimborso della somma con detrazione della franchigia.

Nelle proprie controdeduzioni, l'intermediario chiede il rigetto del ricorso, eccependo quanto segue:

- la ricorrente era intestataria di un conto corrente presso l'intermediario con IBAN **948, cui era collegata la carta di debito fisica **9130 e due carte di debito virtuali numero **428 e **7379;
- nel ricorso dichiara di essere rimasta vittima di una frode, disconoscendo n. 4 operazioni di pagamento per un importo complessivo pari ad € 14.410,00;
- l'intermediario ha rimborsato l'importo di € 2.990,00 su un altro conto corrente, designato in fase di gestione del reclamo preventivo dalla ricorrente;
- rispetto alla descrizione dei fatti presente nel ricorso, si precisa che la ricorrente non era stata contattata da un numero verde riconducibile ad altro intermediario, come confermato dalla denuncia (nella quale afferma di essere stata contattata da un'utenza mobile privata);
- in ogni caso, non è stato allegato alcuno *screenshot* della chiamata ricevuta;
- la ricorrente accedeva al proprio conto corrente tramite App installata sul proprio dispositivo mobile associato al conto e, come indicato nella denuncia, autorizzava personalmente le operazioni sul sito B**, ritenendo di mettere in sicurezza lo stesso conto;
- conclusa la chiamata e appurata la frode, la ricorrente contattava l'intermediario B per chiedere la revoca dei bonifici istantanei disposti sul proprio conto **948, senza successo;
- contattava inoltre il Servizio Clienti dell'intermediario convenuto, che metteva in sicurezza il c/c;
- dalla ricostruzione dei fatti prospettata dalla ricorrente emerge la presenza di indici di colpa grave a lei imputabili, avendo fornito la propria collaborazione attiva al perfezionarsi della frode;
- la truffa subita dalla ricorrente rientra nelle tipologie del c.d. *smishing* e del *vishing*, modalità non sofisticate di truffa per costante giurisprudenza ABF;
- la stessa ricorrente ammette di aver autorizzato trasferimenti di denaro all'interno dell'App di HB dell'intermediario, dopo aver alimentato il proprio conto tramite n. 5 bonifici per un importo complessivo di € 14.418,00, disposti dal conto corrente radicato presso l'intermediario B;

- l'interlocutore si era qualificato come dipendente dell'intermediario B, non di quello convenuto;
- l'SMS civetta, pur contenendo la denominazione dell'intermediario convenuto, non era confluito in una precedente catena di messaggi genuini e presentava evidenti errori di sintassi, alternando, in un'unica frase, un tono formale e informale, rivolgendosi alla ricorrente tramite la seconda e la terza persona singolare;
- le notifiche push ricevute, che rinviano all'App di HB, riportavano il nome del beneficiario e il relativo importo oltre ad un beneficiario sconosciuto;
- la ricorrente ammette di aver condiviso le proprie credenziali di accesso al conto con il frodatore (password e l'indirizzo e-mail personale), essendo verosimile ritenere che la stessa abbia condiviso anche il codice OTP ricevuto via SMS;
- quale ulteriore elemento di colpa grave, la ricorrente ha ordinato il rilascio di ulteriori n. 2 carte di debito virtuali, sulle quali sono state addebitate n. 2 operazioni, rispettivamente dell'importo di € 4.990,00 ed € 1.530,00;
- tali transazioni, impostate on-line dal frodatore, sono state autorizzate nella APP dalla ricorrente tramite il sistema multifattoriale;
- risulta dunque la riconducibilità delle operazioni, oggetto del presente procedimento, alla ricorrente;
- l'intermediario adotta sistemi informatici che rispettano i più alti standard di sicurezza, predisponendo un sistema di autenticazione forte sia per l'accesso all'HB, tramite la propria applicazione mobile o nel sito web, sia per l'autorizzazione delle operazioni dispositive;
- non si è verificato alcun "*data breach*", poiché il nominativo e l'utenza telefonica della ricorrente possono essere stati oggetto di furto in altre circostanze;
- l'intermediario, da tempo, ha intrapreso una capillare serie di campagne informative finalizzate a rendere edotta la propria clientela su truffe analoghe a quella oggetto di ricorso;
- in particolare, alla cliente sono state inviate n. 6 distinte mail nelle date del 14.05.2020, 09.102020, 13.11.2020, 26.10.2021 e del 10.06.2022, oltre a messaggi visibili all'interno della App.

Successivamente, in sede di repliche, la ricorrente, richiamati i propri scritti, insiste nell'accoglimento del ricorso precisando ulteriormente che:

- non appena avuta notizia delle operazioni in uscita dal proprio conto corrente, si è immediatamente attivata presentando la denuncia il 09.01.2023 e dandone comunicazione al servizio clienti della Banca;
- secondo il Collegio di Coordinamento (decisione n. 22745/20) l'"sms *spoofing*" rientra tra le truffe potenzialmente "sofisticate";
- la cronologia delle notifiche push trasmesse dalla Banca non può dirsi idonea a provare una condotta negligente della ricorrente;
- al contrario, è evidente che i truffatori si siano inseriti nel sistema informatico dell'intermediario, modificando i dati della cliente, tra i quali il numero telefonico;
- l'intermediario non è in grado di provare l'effettiva percezione delle notifiche, non avendo la cliente ricevuto alcun sms alert o notifica push delle operazioni contestate;
- le operazioni disconosciute sono risultate, inoltre, anomale secondo quanto risulta dallo stesso sistema di sicurezza della banca;
- infatti, a pagina 5 dell'allegato 5 controdeduzioni è riportato che le operazioni truffaldine erano state individuate dal sistema come caratterizzate da "*high risk score above threshold*" e, pertanto, dovevano essere bloccate dall'intermediario;

- l'Intermediario allude genericamente ad una presunta collaborazione della cliente con il truffatore, senza fornire alcun elemento probatorio;
- l'assenza di tale collaborazione non può essere provata dalla ricorrente, trattandosi di una prova negativa;
- a pagina 6-7 delle controdeduzioni, l'intermediario afferma che il frodatore è penetrato nell'area cliente della ricorrente, procedendo da lì a disporre le operazioni in uscita, previa modifica del telefono cellulare associato al conto corrente;
- conseguentemente, se il sistema informatico dell'Intermediario non si fosse dimostrato permeabile all'intrusione, le operazioni fraudolente non avrebbero potuto avere luogo;
- l'intermediario è tenuto ad adottare tutte le "misure idonee a garantire la sicurezza del servizio" (Cass., n. 13777/2007);
- quanto allegato nelle controdeduzioni non prova la riconducibilità delle operazioni alla cliente, né esclude eventuali anomalie nei sistemi di allerta predisposti dall'Istituto bancario;
- la truffa subita evidenzia un'operatività anomala, in quanto l'importo complessivo delle operazioni truffaldine risulta superiore al consueto ammontare delle operazioni usuali;
- lo stesso intermediario ammette che i device utilizzati dai frodatori erano incompatibili con quelli usualmente utilizzati dalla cliente;
- dai log si evince che gli accessi truffaldini sono stati realizzati da utenti denominati "*goldfish*", modificati a priori per penetrare nel sistema dell'Intermediario, così come l'indirizzo IP relativo all'accesso truffaldino risulta anomalo e incompatibile con quelli solitamente utilizzati dalla ricorrente;
- non vi è prova che le campagne informative dell'intermediario abbiano raggiunto in modo specifico il cliente.

L'intermediario, per contro, in sede di controrepliche, espone quanto segue:

- anche alla luce delle repliche trasmesse, il ricorso risulta infondato in fatto e in diritto;
- la vicenda oggetto di ricorso riguarda un'ipotesi di *smishing* misto a *vishing*, non di *spoofing* come ritenuto erroneamente da parte ricorrente;
- in ogni caso, lo *spoofing* è una variante non particolarmente sofisticata del *phishing* tradizionale (cfr. Coll. Bologna, decisione n. 21451/2021);
- il carattere anomalo delle richieste avrebbe dovuto indurre la cliente a non seguire le indicazioni del finto operatore che, peraltro, si era presentato come funzionario di una banca diversa (cfr. Coll. di Roma, decisione n. 11043/2021);
- non sono attendibili le indicazioni ricevute da un soggetto presentatosi come dipendente di un altro intermediario, che impartiva istruzioni sulla sicurezza di un conto corrente diverso, peraltro chiedendo di effettuare una serie di operazioni di trasferimento di denaro a un terzo;
- le operazioni di pagamento in esame sono pagamenti autorizzati, essendo stati disposti personalmente dalla ricorrente;
- nel corso della frode la cliente ha mantenuto l'esclusivo controllo dell'App di HB installata sul proprio dispositivo mobile;
- la cliente, se fosse stata diligente, avrebbe dovuto procedete al blocco della carta fisica e rifiutare categoricamente il rilascio delle carte virtuali;

- le n. 3 operazioni di pagamento oggetto di ricorso non sono imputabili ad eventuali falle nella sicurezza dell'infrastruttura informatica della Banca, essendo state autorizzate all'interno dell'area riservata del conto della cliente;
- l'intermediario ha provato che le notifiche push e gli SMS contenenti i codici OTP di verifica per l'accesso al conto, condivisi con il frodatore, sono stati correttamente inviati all'utenza telefonica della ricorrente;
- dalla documentazione allegata al ricorso non risulta una compromissione della linea telefonica della ricorrente;
- i sistemi della Banca sono in linea con gli standard richiesti dalla normativa nazionale ed europea;
- nonostante il frodatore avesse effettuato l'accesso al conto dal proprio dispositivo non associato, la cliente non ne aveva perso il possesso, potendovi accedere ed autorizzare le operazioni in parola direttamente dall'App di HB installata in maniera esclusiva sul proprio device;
- proprio a fronte dell'elevato importo di ciascuna delle operazioni contestate, i sistemi hanno richiesto l'autorizzazione tramite sistema multifattoriale;
- qualora l'intermediario adotti un efficiente sistema di sicurezza informatica, non risponde del *phishing* avvenuto ai danni dei propri clienti (Cass. civ., Sez. I, 13.03.2023, n. 7214);
- da quanto prodotto nelle controdeduzioni risulta che la Banca ha provato l'invio di mail informative direttamente all'indirizzo di posta elettronica della ricorrente, con cadenza regolare nel corso dell'intero rapporto di conto corrente e avvisi visualizzabili all'interno dell'App di HB.

## DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto la contestazione di n. 3 operazioni bancarie dell'importo complessivo di € 11.420,00, effettuate in data 03.01.2023.
Si tratta, nello specifico, di n. 3 pagamenti rispettivamente dell'importo di € 4.900,00, € 4.990,00 ed € 1.530,00, a favore dell'esercente "B**".
Si evidenzia che, nel medesimo contesto truffaldino, è stata eseguita una quarta operazione da € 2.990,00, non oggetto di ricorso in quanto rimborsata dall'intermediario (come affermato delle parti).
Le operazioni sono state eseguite con provvista sul conto derivante da bonifici istantanei, eseguiti nel medesimo contesto truffaldino da un c/c intestato alla medesima cliente presso altro intermediario (non convenuto) e mediante addebito sulle carte n. ***9130, ***8428 e ***1879.
Alla data delle operazioni 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.
In merito alle modalità di esecuzione delle operazioni contestate, l'intermediario afferma che le verifiche effettuate avrebbero accertato la legittima esecuzione e sostanziale regolarità delle operazioni contestate.
Nel caso di specie, la truffa si è articolata in n. 3 operazioni di pagamento (oltre ad un'ulteriore operazione non contestata, in quanto rimborsata).
Tali operazioni sono state precedute dalle seguenti azioni preliminari poste in essere dal truffatore:

- accesso al conto da device diversi da quello usuale;
- reazione di n. 2 carte di pagamento virtuali.

Quanto al Login, l'intermediario afferma che la procedura di accesso si basa sull'uso di due o più fattori consistenti nell'utilizzo dell'applicazione mobile installata sul dispositivo associato in via esclusiva al titolare del conto, con inserimento delle credenziali personali, costituite dal proprio indirizzo e-mail registrato e dalla password personale oppure richiedendo in aggiunta un codice SMS, inviato esclusivamente all'utenza telefonica presente in anagrafica.
In alternativa, l'utente può accedere al proprio conto tramite il sito web della Banca (c.d. Web-App), attraverso conferma dell'accesso per mezzo dell'applicazione mobile installata sul dispositivo associato in via esclusiva.
Quanto all'operatività disconosciuta, afferma invece che:

- il truffatore ha predisposto le n. 3 operazioni oggetto di ricorso autonomamente, attraverso l'inserimento di tali dati su portali web terzi per poi indurre la ricorrente, nel corso della telefonata, ad autorizzare le suddette operazioni;
- le operazioni di pagamento controverse sono state predisposte dal frodatore a distanza, in quanto costituivano delle transazioni c.d. "card not present" (CNP).

In merito all'autenticazione forte – SCA – nella fase di accesso all'App (login), l'intermediario produce evidenze da cui risulta che ciascun login, compreso quello effettuato con un nuovo device, è stato effettuato con sistema di autenticazione a doppio fattore.
Con riferimento alle n. 3 operazioni di pagamento, invece, l'intermediario rileva che le stesse sono state avviate direttamente dal truffatore, il quale, dopo aver ottenuto il totale accesso al conto corrente, è riuscito a creare 2 carte di debito virtuali.
In merito alla procedura di creazione delle carte virtuali, tuttavia, l'intermediario non

specifica le modalità. Da quanto prodotto, ai fini della SCA non sembra possibile ricavare alcun elemento di autenticazione.
Inoltre, con riferimento alle operazioni di pagamento, l'intermediario afferma che sarebbero state disposte dai truffatori tramite il sito web del merchant e, quindi, correttamente autenticate in-app dalla Ricorrente medesima; sarebbero state tutte "Challenged" e "Confirmed", ovvero autenticate secondo il protocollo di sicurezza M** SecureCode a fronte della convalida delle relative richieste di addebito pervenute in-app tramite notifica push sul dispositivo mobile personale della Ricorrente associato al conto.
Alla luce di quanto in atti, risulta possibile rilevare che, nonostante l'intermediario affermi che le operazioni contestate siano state autorizzate con sistema multifattoriale, le evidenze prodotte dimostrano il solo elemento di possesso (notifica push e successiva autorizzazione in app) ma non anche il secondo necessario elemento di conoscenza o di inerenza necessario ai fini della SCA.
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 € 11.420,00.**
**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