COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore DANIELE PERSANO

Seduta del 05/12/2024

FATTO

Nel presente procedimento, la parte ricorrente afferma quanto segue:

- in data 05/07/2023, venivano effettuati 4 bonifici dal c/c n. ***695 in essere presso l'intermediario convenuto e intestato alla ricorrente e alla di lei figlia;
- le 4 operazioni sono state effettuate nell'arco di pochi minuti, tra le ore 13:55 e le ore 14:01, per un ammontare complessivo di € 49.770,00, a favore di un terzo sconosciuto;
- non riceveva alcuna chiamata da parte del servizio dell'intermediario *Securecall* per autorizzare le operazioni via *internet banking*;
- poco dopo le ore 15:00, si accorgeva di 4 chiamate senza risposta, provenienti dal numero di telefono della direttrice della propria filiale di riferimento;
- la cliente richiamava il citato numero e le rispondeva un uomo che affermava di aver chiamato per conto della direttrice della filiale e che spiegava di aver notato operazioni sospette;
- la cliente negava di aver autorizzato alcuna operazione dal conto della madre e di aver divulgato codici o credenziali; veniva rassicurata dall'interlocutore che si sarebbe occupato della questione;

- la telefonata terminava e, in seguito, la cointestataria riceveva un'altra telefonata dallo stesso numero: a chiamare era la stessa direttrice della filiale, la quale negava di aver effettuato la telefonata chiusa poco prima;
- la direttrice la informava che i bonifici effettuati erano stati rilevati dal servizio antifrode e che, tuttavia, non era stato possibile bloccare i citati bonifici, dal momento che erano stati disposti a favore di un conto acceso presso lo stesso intermediario convenuto;
- per motivi di sicurezza erano quindi stati bloccati tutti i conti correnti ai quali era possibile accedere tramite l'utenza della cointestataria;
- procedeva a presentare denuncia presso le Autorità di Pubblica Sicurezza insieme alla madre;
- presentava reclamo all'intermediario in data 06/07/2023 e, successivamente, in data 10/07/2023 preso la filiale, tramite firma dei moduli di disconoscimento: in quell'occasione, le clienti provavano a riattivare l'utenza online e si accorgevano che i dispositivi autorizzati alla conferma delle operazioni erano due, di cui uno ignoto che la cointestataria rimuoveva su consiglio della direttrice della filiale;
- seguivano ulteriori comunicazioni con l'intermediario relative all'utenza online;
- in data 31/07/2023 la cointestataria riceveva la risposta negativa della banca alla richiesta di disconoscimento;
- le clienti inviavano un nuovo reclamo, anch'esso riscontrato negativamente dalla banca;
- la somma che la banca è riuscita a richiamare è irrisoria;
- sussiste la responsabilità della banca per non aver sospeso le operazioni dalla stessa banca rilevate come sospette;
- i procuratori legali delle clienti hanno presentato ulteriore diffida sostenendo che l'accaduto fosse da ricondurre ad un'ipotesi di *data breach* del data base della banca; anche tale diffida è stata riscontrata negativamente;
- la banca afferma che si tratta di una truffa di *spoofing* nel tentativo di spostare la responsabilità del danno sulle clienti, quando, in realtà, nessun soggetto terzo si è presentato quale interlocutore attendibile per ottenere codici finalizzati alla disposizione dei bonifici;
- i fatti oggetto della presente vicenda rientrano nell'ipotesi di *data breach* della banca dati della banca.

La ricorrente chiede, dunque, all'Arbitro, di accertare il proprio diritto ad ottenere il rimborso dell'importo che ritiene essergli stato fraudolentemente sottratto pari ad € 49.770,00.

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

- è la stessa cointestataria/figlia della ricorrente ad ammettere, in diversi passaggi, di aver ricevuto gli sms alert, pur non avendo avuto la possibilità di prendere visione in tempo reale;
- l'operatività che ha consentito *ab origine* la frode è stata condotta dall'utenza telefonica della cointestataria/figlia della ricorrente;
- la telefonata di ingaggio risultava provenire da un numero non riconducibile alla banca: trattasi di episodio riconducibile al *vishing*, probabilmente congiunto a *smishing*, in cui i frodatori si sono finti addetti antifrode della banca;
- la banca ha inviato diverse comunicazioni volte a mettere in guardia la propria clientela dal rischio delle frodi informatiche;

- le operazioni disconosciute dalle ricorrenti sono state disposte ed autorizzate mediante le credenziali dispositive e autorizzative rilasciate, previo *enrollment* di un nuovo dispositivo;
- la banca ha inserito le *recall* per le operazioni in uscita non appena ricevuto notizia della frode;
- la truffa è avvenuta per colpa grave della delegata della ricorrente e per omessa custodia degli strumenti e delle credenziali messe a sua disposizione dalla banca;
- non sono state riscontrate intrusioni nei propri sistemi informatici, né sussistono altri profili di responsabilità adducibili a carico della banca.

Successivamente, la cliente, in sede di repliche, richiamati i propri scritti, precisa ulteriormente che:

- il solo fatto di aver qualificato l'evento occorso con quattro fattispecie diverse (*social engineering* nella forma del *phising, vishing, smishing* e *spoofing*) è sufficiente a rendere palese che l'intermediario non è certo di quanto sia accaduto;
- l'evento non è riconducibile al *phishing* o allo *smishing*, dal momento che le operazioni bancarie disconosciute sono state realizzate senza la previa ricezione di email/sms civetta o chiamate in cui hanno fornito le credenziali di sicurezza, per altro, mai comunicate a nessuno;
- non è riconducibile nemmeno al *vishing* perché la ricorrente ha chiamato il numero della direttrice della filiale quando ormai le operazioni erano state compiute; a quel numero ha risposto un uomo che ha affermato di aver chiamato per conto della direttrice e, in ogni caso, la cliente non ha comunicato alcun dato sensibile;
- la truffa è stata quindi realizzata violando i sistemi di sicurezza propri dell'istituto bancario, come emergerebbe dal fatto che la cliente non ha ricevuto alcuna chiamata *secure call* per *l'enrollment* avvenuto il 21/06/2023 o dal fatto che l'sms relativo all'*enrollment* di un altro *device* non è mai stato ricevuto dalla cliente;
- ad ogni modo non si ha contezza del modo in cui la documentazione informatica sia stata elaborata e dunque risultano inattendibili i file prodotti dall'intermediario;
- gli elementi costitutivi delle ipotizzate tecniche di *social engineering* non si rinvengono nemmeno nell'ambito delle disposizioni bancarie poste in essere il 05/07/2023, dal momento che, nel periodo antecedente, le ricorrenti non hanno ricevuto chiamate o mail "civetta" e non hanno comunicato a nessuno le proprie credenziali né cliccato alcun link;
- l'intermediario non ha contestato alcun comportamento fraudolento in capo alle ricorrenti, peraltro, in alcun modo ravvisabile: le ricorrenti non hanno mai comunicato a terzi le credenziali di accesso a tale servizio e l'intermediario non ha fornito alcuna evidenza contraria al riguardo;
- richiama gli obblighi previsti a carico dell'intermediario ai sensi del d.lgs. 11/2010 e rileva che l'intermediario non ha dato prova di aver assicurato che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi né che le operazioni siano state correttamente registrate e contabilizzate;
- l'intermediario ha sollevato una contestazione in merito alla chiamata fatta dalla cliente al numero di telefono della direttrice, elemento che non ha inciso in alcun modo sugli eventi in quanto avvenuto successivamente alla esecuzione dei bonifici contestati;
- non sussiste alcuna colpa grave nemmeno in merito alla tardiva presa visione degli sms alert, dal momento che la stessa banca riferisce che le somme sono state immediatamente trasferite verso altri conti correnti;

- in ogni caso, l'sms alert rappresenta una tutela *ex post* che non esonera l'intermediario dalla predisposizione di servizi di protezione avanzati, atti a prevenire il compimento stesso della frode;
- inoltre, la prova incombente sull'intermediario va letta in combinato disposto con il principio generale dall'art. 1218 c.c. che impone all'intermediario di provare di aver adempiuto agli obblighi di custodia e salvaguardia delle somme dei clienti con la diligenza del buono e accorto banchiere;
- nel caso di specie, si ravvisano gravi negligenze della banca, come evidenziano i log prodotti in cui non è stata posta in essere alcuna SCA relativamente all'accesso del 21/06/2023; la banca, inoltre, non si è premurata di verificare la corretta ricezione dell'sms che comunica l'*enrollment* di un altro dispositivo e che avrebbe permesso alla cliente di bloccare l'abilitazione e impedire il verificarsi dell'evento;
- la più grave negligenza dell'intermediario consiste nel non aver ritenuto sospette e non aver bloccato le disposizioni contestate: le ricorrenti non avevano mai effettuato alcuna disposizione sul conto bancario violato;
- ritiene piuttosto che l'evento sia riconducibile ad un caso di *man in the browser*, evento particolarmente insidioso in cui, l'appropriazione indebita dei codici di sicurezza, avviene attraverso un meccanismo particolarmente insidioso.

L'intermediario, nelle proprie controrepliche, riportandosi alle conclusioni in atti, controreplica che:

- non ha effettuato alcuna qualificazione, ma si è limitato ad individuare le diverse tecniche utilizzate dai truffatori per ottenere il loro scopo; in ogni caso, non sono presenti agli atti evidenze degli eventuali sms ricevuti dalla cliente;
- non corrisponde al vero che le clienti non abbiano ricevuto alcuna chiamata, come dimostrerebbero i log da cui si evince che si è conclusa con successo la chiamata *secure call* ricevuta sul numero ***377, univocamente associato alla ricorrente;
- dalla rubrica aziendale non risulta alcun riferimento al numero privato della direttrice di filiale: il fatto che sul cellulare della ricorrente il numero sia salvato con il nome della direttrice non vuol dire necessariamente che la cosa sia vera;
- non vi è stata alcuna violazione dei sistemi di sicurezza dell'istituto, come dimostrano gli allegati relativi al *login* antecedente all'*enrollment* e all'*enrollment* stesso; il dispositivo dormiente è stato poi utilizzato per eseguire le operazioni senza che i frodatori avessero bisogno di contattare nuovamente la cliente;
- l'ipotesi che nel caso di specie si sia verificato un *man in the browser* implicherebbe l'ammissione che la cliente abbia inserito l'operazione e che l'IBAN sia stato modificato a causa di un malware sul pc;
- la banca non può dimostrare se e come la cliente abbia fornito le credenziali; risulta tuttavia provato che l'accesso e *l'enrollment* sono stati eseguiti da soggetti che erano a conoscenza delle credenziali e mediante numero certificato.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto la contestazione di n. 4 operazioni bancarie non autorizzate dell'importo complessivo di € 49.770,00, effettuate in data 05/07/2023.

Nello specifico si tratta delle seguenti operazioni:

1) h. 13:55 - € 14.950,00
2) h. 13:57 - € 14.940,00

3) h. 13:59 - € 14.900,00
4) h. 14:01 - € 4.980,00

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 quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

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.

Sulla base di quanto affermato dall'intermediario nelle controdeduzioni, è possibile rilevare che le operazioni contestate sono state disposte tramite APP e che, due settimane prima della frode, è stato effettuato *l'enrollment* dell'APP su numero certificato.

L'intermediario descrive, inoltre, quanto segue:

- per il *login* in App è necessario inserire un (i) codice utente o alias, (ii) una "data importante" (impostata in fase di primo accesso) e (iii) un PIN dispositivo;
- il PIN dispositivo viene impostato in fase di attivazione del servizio *Secure Call*, servizio che comporta la ricezione di una chiamata al numero di telefono associato all'utente (fattore di possesso) e contestuale inserimento del PIN dispositivo;
- in seguito all'accesso, il completamento dell'*enrollment* viene autorizzato tramite il sistema di *secure call* attivo sul numero certificato e con digitazione del PIN noto esclusivamente all'utente.

Dall'analisi delle evidenze prodotte dall'intermediario si rileva che, per la fase di login, dai log prodotti non risulta possibile riscontrare evidenza della digitazione del PIN dispositivo, fattore di conoscenza che l'intermediario afferma essere necessario per il *login* (cfr. al riguardo, la voce "N/A" in corrispondenza del *login* immediatamente antecedente *all'enrollment*).

Tuttavia, è lo stesso intermediario a precisare che per questa specifica fase non è ancora performata la SCA, non essendovi accesso al servizio ma dovendosi prima procedere all'enrollment del dispositivo.
Con riferimento all'enrollment si riscontra evidenza della *secure call* effettuata al numero di telefono corrispondente a quello indicato dalla cointestataria come proprio – fattore di possesso.
Si evidenzia altresì che la chiamata ha richiesto l'inserimento del PIN ("*registra il tuo dispositivo […] per l'accesso all'app e all'home banking. Inserisci il pin dispositivo seguito dal tasto cancelletto*").
Si osserva che l'enrollment è avvenuto tramite inserimento, nell'ambito della *Securecall* al *device* (fattore di possesso), del PIN dispositivo necessario (fattore di conoscenza) all'enrollment dell'APP.
Si rammenta per completezza che la ricorrente nega di aver ricevuto la chiamata *Securecall* in data 21/06/2023.
Con riferimento, infine, all'accesso antecedente alla disposizione dei bonifici contestati, l'intermediario afferma che alle ore 13:46 del 05/07/2023 è stato effettuato un *login* mediante inserimento del PIN dispositivo all'interno dell'APP ufficiale dell'intermediario.
Produce evidenze da cui si rileva che è stato effettuato un accesso alle ore 13:46 del 05/07/2023 dallo stesso utente che ha effettuato l'*enrollment* in data 21/06/2023.
L'intermediario afferma che le operazioni contestate sono state autenticate tramite *"PIN dispositivo all'interno dell'App ufficiale".*
Al riguardo l'intermediario produce evidenze, dalla cui analisi non sembrerebbe possibile riscontrare evidenza dell'effettivo inserimento del PIN.
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 € 49.770,00.
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
ANDREA TINA