COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) CORNO	Membro di designazione rappresentativa degli intermediari
(MI) COLOMBO	Membro di designazione rappresentativa dei clienti

Relatore (MI) COLOMBO

Seduta del 19/12/2024

FATTO

La società ricorrente, titolare di un contratto avente ad oggetto la prestazione di servizi di pagamento con l'intermediario convenuto, espone di essere stata vittima di una frode informatica, a seguito della quale ha subito la perdita della somma di € 26.503,10, di cui € 3,10 in virtù delle commissioni applicate.

La truffa viene descritta nei seguenti termini:
- in data 25 giugno 2024 la propria legale rappresentante avrebbe ricevuto un SMS, a suo dire riconducibile ad un intermediario terzo, non convenuto nella presente sede, che l'avvisava di un pagamento di € 789,00;
- ella avrebbe contattato, a quel punto, il numero di telefono dell'assistenza indicato nel menzionato SMS, per bloccare il pagamento;
- seguendo le istruzioni del sedicente operatore bancario, avrebbe aperto il *link* contenuto nel messaggio nel frattempo ricevuto ed accedeva alla piattaforma ***, riferibile all'intermediario convenuto, ove avrebbe riscontrato la presenza di tre disposizioni effettuate a favore di beneficiari a lei ignoti;
- la legale rappresentante della ricorrente non avrebbe comunicato al proprio interlocutore né il codice utente, né il PIN;

- in seguito, ella avrebbe autorizzato tramite OTP alcune operazioni, che a detta dell'operatore sarebbero servite ad annullare le disposizioni, ed avrebbe concluso la telefonata;
- non avendo ricevuto alcun SMS di conferma, si sarebbe insospettita e, controllando il conto *on-line*, si sarebbe accorta dell'ammanco;
- contattato immediatamente l'intermediario, chiedeva il blocco dei due bonifici disconosciuti che aveva rilevato, rispettivamente di € 12.500,00 e di € 14.000,00;
- la ricorrente avrebbe poi sporto denunzia e presentato reclamo, al quale l'intermediario rispondeva negativamente.

Sulla base di queste premesse in via di fatto, la ricorrente deduce la responsabilità dell'intermediario convenuto e conclude per il rimborso della somma sottratta.

Nelle proprie controdeduzioni la parte convenuta eccepisce anzitutto che la cliente avrebbe ammesso di avere materialmente eseguito le operazioni di pagamento, sia pure a causa di una frode perpetrata da terzi (c.d. operazioni sotto dettatura).
Peraltro, le operazioni risulterebbero essere state autorizzate tramite il *token* in uso dalla cliente, mentre la *chat* telefonica prodotta è riconducibile ad un diverso intermediario.
In considerazione di tali circostanze, l'intermediario ravvisa la sussistenza di colpa grave in capo alla cliente e conclude per il rigetto del ricorso.

In sede di replica, la ricorrente rileva come la parte convenuta non abbia fornito alcuna spiegazione circa la mancata ricezione degli SMS di inserimento di un nuovo beneficiario e di esecuzione dei bonifici. Invero, se avesse ricevuto un SMS al primo bonifico si sarebbe accorta della truffa e si sarebbe a quel punto fermata, così evitando quanto meno il danno cagionato in conseguenza del secondo.
In ogni caso, precisa di avere sì autorizzato le operazioni (credendo erroneamente di annullarle), ma nega recisamente di averle predisposte.
Insiste, dunque, affinché il ricorso venga accolto.

L'intermediario non ha controreplicato.

DIRITTO

Rileva preliminarmente il Collegio che, sulla scorta della documentazione in atti, non è possibile stabilire con precisione l'orario esatto delle disposizioni disconosciute.
Sulla scorta dei *log* prodotti dall'intermediario, risultano infatti tre bonifici (e non due), collocati tra le ore 16:28 e le ore 16:46 del 25 giugno 2024, in un lasso di tempo dunque compatibile con quello della riferita truffa. Il fatto che i *log* non contengano indicazioni relative all'importo non consente di comprendere, come detto, quali siano stati gli esatti orari in cui furono effettuate le due disposizioni oggetto del presente contenzioso.

Tanto premesso, occorre in primo luogo delibare l'eccezione dell'intermediario, relativa al fatto che vi sarebbe nel caso di specie la prova dell'avvenuta esecuzione materiale delle operazioni contestate da parte della cliente, con conseguente inapplicabilità della disciplina della c.d. S.C.A. (*Strong Customer Authentication*, o autenticazione forte).
A riguardo, ritiene il Collegio che, nel caso in esame, i bonifici siano stati predisposti materialmente dal truffatore ed autorizzati grazie alla cooperazione inconsapevole della

ricorrente, la quale ha ammesso di avere inserito certamente almeno uno dei fattori di autenticazione.
Le tracciature informatiche prodotte dall'intermediario non sono peraltro di particolare aiuto, ai fini della ricostruzione compiuta della vicenda, in quanto non vi si individua puntualmente nemmeno l'orario del *login* prodromico all'esecuzione delle operazioni, né il dispositivo da cui è stato effettuato (se da *App* installata sullo *smartphone* della cliente, o da *web*), e neppure – come già detto – l'orario preciso di esecuzione delle operazioni contestate.

L'ipotesi più plausibile, che il Collegio ritiene essersi verificata, è dunque la seguente:
- alle ore 16:20 del 25 giugno 2024 veniva ricevuto dalla legale rappresentante della ricorrente un SMS contenente, oltre alla denominazione di altro intermediario, anche un *link*, sul quale ella cliccava ed aveva così accesso, apparentemente, alla piattaforma ***, riferibile all'intermediario convenuto;
- in realtà il *link* dava accesso ad un sito clone, sul quale erano state caricate delle disposizioni fasulle;
- sulla scorta delle tracciature in atti, a partire dalle ore 16:20 si evincono diversi *login*, i primi dei quali da *web*, e che pertanto potrebbero essere stati effettuati anche dal truffatore, mentre altri risultano essere stati effettuati dal dispositivo mobile di cui usualmente si serviva la ricorrente;
- tra questi *login*, solo due sono seguiti da operazioni di bonifico (quello delle ore 16:27 e quello delle ore 16:46) ed entrambi sono stati effettuati da *web*;
- dunque, le operazioni contestate ben potrebbero essere state predisposte dal frodatore tramite collegamento *web* al conto corrente *on-line* della cliente, mediante inserimento del codice utente e PIN carpiti attraverso il sito clone direttamente dal truffatore, e successivo OTP autorizzato dalla cliente.

Ebbene, come recentemente stabilito dall'unanime indirizzo dei Collegi, l'operazione di pagamento *on-line* preparata dal truffatore ed autorizzata dal cliente tramite la ricezione della notifica *push* e l'inserimento della biometria, o di un codice di conferma, non può ritenersi eseguita per intero dal pagatore, come viceversa necessario per escludere il regime di responsabilità previsto dalla PSD2 e dalla disciplina interna di recepimento (cfr., a riguardo, Coll. Bologna n. 7079/24; Coll. Palermo n. 9033/24).
Ne consegue che nel caso in esame deve trovare applicazione la già menzionata disciplina della c.d. S.C.A. (*Strong Customer Authentication*, o autenticazione forte), la quale si realizza con il ricorso ad almeno due dei seguenti tre fattori: *(i)* conoscenza; *(ii)* inerenza; *(iii)* possesso. Tali elementi debbono essere reciprocamente indipendenti e appartenere a categorie diverse.
L'autenticazione forte è richiesta sia nella fase di accesso al conto (*login*), o di *enrollment* dell'*App* su un *device*, o di registrazione della carta su un *wallet*, sia nella fase di esecuzione delle singole operazioni.
È inoltre unanime l'indirizzo dei Collegi, a mente del quale la prova dell'avvenuta autenticazione in modo *compliant* rispetto alla disciplina di settore deve essere prioritariamente fornita dall'intermediario, rispetto a quella avente ad oggetto la sussistenza di colpa grave in capo al cliente.
In altri termini, se l'intermediario non fornisce la suddetta prova prioritaria, il ricorso deve essere accolto, anche se – in ipotesi – vi fosse agli atti la prova della colpa grave del cliente.

Venendo al caso in esame, ritiene il Collegio che l'intermediario non abbia idoneamente assolto al richiamato onere probatorio, su di esso gravante in via prioritaria.
Iniziando l'analisi dalle azioni antecedenti all'esecuzione delle operazioni contestate, deve essere anzitutto ribadito che l'intermediario nulla specifica in merito al *login* al conto corrente prodromico alle stesse, né riguardo all'orario, né riguardo ai fattori di autenticazione utilizzati.
Le evidenze prodotte consistono nell'elenco degli accessi del 25 giugno 2024, nel *file* di *log* in formato tabella con legenda esplicativa e nel dettaglio del *token* che consente di generare codici OTP inserendo i codici mostrati su pc e il proprio PIN.

In merito a detta documentazione si rileva quanto segue:
- i *log* integrali sono parziali (vi è un'unica sequenza, delle ore 16:15);
- risultano due accessi al conto corrente del tipo "*Login Forte*", seguiti dall'esecuzione di operazioni di bonifico: il primo è avvenuto alle ore 16:27 e il secondo alle ore 16:45 del 25 giugno 2024;
- entrambi risultano preceduti dalla dicitura "*Login con successo*", realizzato con codice utente e PIN al medesimo orario;
- entrambi risultano autenticati con OTP standard generato tramite *push* (validazione del messaggio ricevuto sul *token software* tramite PIN o biometria);
- come già detto, risultano effettuate tre, e non due operazioni di bonifico.

Nel caso in esame, i fattori in concreto utilizzati per autorizzare i due *login* potrebbero essere il PIN e l'OTP; senonché, in assenza di spiegazioni a riguardo dell'intermediario, bisognerebbe presumere che "*Login con successo*" e "*Login forte*" appartengano alla stessa sessione di *login*, ma tale presunzione non viene ritenuta dal Collegio sussistere, in quanto mancante dei requisiti di cui all'art. 2927 c.c., sicché – in virtù della riferita lacuna nell'esplicazione da parte dell'intermediario – deve concludersi che manchi, già per la fase prodromica, la prova dell'adozione di un sistema conforme alla S.C.A.
Peraltro, a non diversa conclusione deve pervenirsi anche con riferimento alla fase dell'esecuzione dei bonifici.
Si è invero già detto che l'intermediario non fornisce alcuna indicazione in merito agli orari nei quali sono stati eseguiti i bonifici e/o ai fattori di autenticazione utilizzati, limitatosi essendo ad affermare che essi sono stati eseguiti dal *token* della cliente.
Le evidenze a riguardo fornite consistono nel dettaglio del *token* e nel *file* di *log* con legenda esplicativa.
In merito a detta documentazione si rileva quanto segue:
- come già più volte rilevato, le operazioni di bonifico che si rinvengono sono tre, e non due, e dunque non è possibile individuare con esattezza quali siano le operazioni contestate;
- i bonifici sono stati autorizzati con OTP generato tramite *DATA_ENTRY*, a mezzo del *token* in uso alla ricorrente.
In relazione al secondo fattore di autenticazione, si rammenta che l'EBA ritiene "*riutilizzabile*" il fattore utilizzato per l'accesso all'area riservata (*login*), purché l'azione avvenga nell'ambito della medesima sessione (a riguardo, la Q&A EBA n. 4141/2018), come potrebbe essere accaduto nel caso di specie con il codice PIN.

Senonché, la sopra riferita lacuna probatoria riguardante l'individuazione esatta della sessione (o delle sessioni) di *login*, antecedente (o antecedenti) alle disposizioni fraudolente, non consente di ritenere provata l'autenticazione con doppio fattore neanche relativamente alla fase dispositiva.

La mancata dimostrazione di avere correttamente provveduto all'autenticazione in maniera *compliant* al sistema della S.C.A. espone dunque l'intermediario all'obbligo di rimborsare l'intera operazione fraudolenta, sicché va accolta la domanda intesa al recupero dell'importo sottratto, maggiorato delle commissioni applicate.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 26.503,00.
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