Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) FERRANTE	Membro designato dalla Banca d'Italia
(TO) SETTEMBRE	Membro designato dalla Banca d'Italia
(TO) SPAGNOL	Membro di designazione rappresentativa degli intermediari
(TO) BANI	Membro di designazione rappresentativa dei clienti

Relatore Elisabetta Bani

Seduta del 21/02/2024

FATTO

La parte ricorrente afferma, in sintesi:

- che in data 30.01.2023 è stato effettuato un bonifico fraudolento dell'importo di € 28.500,00 dal conto aperto presso l'intermediario;
- che la gestione del conto corrente è stata da tempo affidata dal Sig. G, Presidente della società, al collaboratore contabile (tutt'ora impiegato della società) Sig. N, e il conto corrente era unicamente collegato e quindi gestito dall'utenza telefonica intestata a quest'ultimo: 333xxxxx92;
- che per effettuare bonifici o altre operazioni bancarie tramite l'home banking, l'unico sistema in uso alla Società all'epoca dei fatti era quello che prevedeva la "*secure call* identificativa";
- che dall'utenza telefonica 333xxxxx92, come emerge dal report della Compagna Telefonica (all.2), non risultano chiamate al numero verde 800xxxx14 in data 30.1.2023, tantomeno alle ore 18:28:11 (ora di effettuazione dell'operazione), per entrare sull'home banking e per concedere l'autorizzazione della disposizione di pagamento della somma di € 28.500,00, per cui la disposizione non può essere stata data dalla Società;
- che l'operazione di bonifico è stata tempestivamente disconosciuta (all.3) tant'è che in data 31.1.2023 l'intermediario inviava ad un indirizzo email presuntivamente

appartenente alla banca beneficiaria una richiesta di recall del bonifico fraudolento, purtroppo con esito negativo (all.3/a);
- di aver presentato denuncia contro ignoti a seguito del quale è stato aperto un procedimento penale presso il tribunale di M;
- che l'intermediario riscontrava negativamente il reclamo asserendo l'assenza di violazioni del proprio sistema di sicurezza;
- di aver chiesto all'intermediario i files dei log relativi all'operazione e gli indirizzi IP dell'operazione e gli IP storici per effettuare un confronto, ma la banca riscontrava la richiesta riferendo che tale documentazione era ad "esclusivo uso interno";
- di aver quindi inviato esposto alla Banca d'Italia per non aver consentito alla Società di effettuare controlli tramite periti informatici al fine di provare la propria estraneità ai fatti;
- che, nonostante il presunto intervento della Banca d'Italia l'intermediario non ha più comunicato alcunché.;

L'intermediario resistente, nelle controdeduzioni, afferma:

- la società ricorrente è titolare, dal febbraio 1996, del conto corrente n. 24/xxxx1 sul quale è stata disposta e disconosciuta l'operazione di bonifico di € 28.500,00 in data 30.01.2023;
- la società ha chiesto di avvalersi del Servizio di internet banking per i clienti corporate, in data 13.06.2013;
- in data 18.12.2019 la società, per il tramite della propria filiale, ha richiesto l'associazione di un nuovo numero telefonico (333xxxxx92) in uso al Sig. G (rappresentante legale della società);
- la parte ricorrente non ha fornito elementi utili a ricostruire la dinamica della frode, essendosi limitata a disconoscere l'operazione di bonifico;
- l'operazione disconosciuta è stata correttamente autenticata tramite sistema a doppio fattore, registrata e contabilizzata senza anomalie sul conto corrente intestato alla società;
- in particolare, la perizia tecnico informatica fornita dall'outsourcer ha dimostrato che l'operazione è stata effettuata con l'inserimento delle password statica e dinamica, e che la chiamata di secure call è stata effettuata al numero associato al conto corrente (333xxxxx92);
- a seguito di controlli sul sistema è emerso che non si sono verificati fenomeni di data breach, né in data 30.01.2023, né in precedenza;
- la parte ricorrente, salvo affermare una ipotetica quanto inverosimile violazione dei sistemi di sicurezza della banca, dichiara di essere stata vittima di una truffa informatica senza tuttavia specificarne le modalità attuative;
- al contrario, la corretta operatività accertata in data 30.01.2023 consente di ritenere che la truffa perpetrata nei confronti della parte ricorrente sia riconducibile al più ampio fenomeno di phishing/vishing, in ragione del fatto che non è stata data prova di un possibile attacco di man in the middle e che il sistema non è stato in alcun modo violato;
- la diffusione di siffatte frodi è ormai estremamente nota;
- ha inviato numerose comunicazioni e messaggi di alert ai propri clienti al fine di renderli edotti in ordine a tali modalità di frode;
- la truffa informatica si è realizzata unicamente grazie alla condotta colposamente collaborativa da parte dell'utilizzatore con i truffa.

Nel replicare alle controdeduzioni, la parte ricorrente ha precisato che:

- la parte resistente ha del tutto omesso di prendere posizione in relazione al fatto che, come emerge dal tabulato della Compagnia telefonica, in data 30.01.2023, non sono state effettuate chiamate in uscita verso il numero verde dedicato per la Secure Call;
- il sistema di sicurezza della banca, all'epoca dei fatti, prevedeva una doppia telefonata da parte dell'utente, con numero in chiaro, verso il numero verde, ma di tale doppia telefonata non vi è traccia;
- evidentemente il sistema della banca non era, quantomeno all'epoca, idoneo a proteggere i conti correnti, tant'è che la modalità di autenticazione è stata in seguito modificata con una chiamata in entrata dal numero verde (e non più una chiamata in uscita verso lo stesso);
- peraltro, l'intermediario per ben due volte afferma che "*il numero chiamato corrisponde a quello associato"* mentre all'epoca della frode il sistema identificativo di sicurezza era quello previgente che, appunto, non prevedeva chiamate in entrata ma in uscita da parte dell'utente;
- l'intermediario contesta la mancata illustrazione delle circostanze utili alla ricostruzione dell'accaduto, ma tutte le informazioni possibili sono già state fornite;
- infatti, nei giorni precedenti la frode non sono state rilevate circostanze anomale e l'operazione è stata rilevata soltanto dopo che era già stata eseguita, e ciò nonostante non fosse stata mai effettuata alcuna chiamata di Secure Call in uscita, unica modalità per poter disporre un bonifico;
- dall'esame del log di cui all'allegato 9, a pagina 2, emerge che l'operazione è stata disposta da IP 176.xxx.xx.xx, IP collegato a Compagnia telefonica diversa da quella di parte ricorrente, mentre l'IP normalmente utilizzato dalla società è un IP statico (109.xxx.xx.xxx).

L'intermediario, nelle controrepliche ha precisato che:

- neppure in sede di repliche la parte ricorrente ha fornito elementi idonei a consentire di ricostruire la dinamica della frode;
- tale circostanza viene considerata dai Collegi come prova indiziaria della colpa grave del cliente;
- dai log informatici è stato comunque possibile ricostruire la dinamica della frode, dalla quale emerge che l'operazione è stata correttamente autenticata tramite il cellulare del ricorrente (oltre che tramite la password statica);
- con riguardato al report telefonico prodotto in atti dalla parte ricorrente, è doveroso segnalare che la crescente offerta di servizi digitali per la comunicazione vocale via web ha portato ad una ampia diffusione di campagne telefoniche di vario genere in cui possono insinuarsi spam e tipologie di truffe identificate come caller id spoofing o fake caller id ovvero tentativi di raggiri telefonici basati sulla falsificazione dell'identità del chiamante solitamente visualizzata sul display del telefono, impersonificando talvolta anche utenze legittime;
- in questo contesto, ancora non sufficientemente tutelato dalla normativa in vigore, i truffatori utilizzano lo spoofing per chiamare da uno specifico numero di telefono simulando di essere l'utente che utilizza la piattaforma della banca;
- in questo complicato contesto la banca non può essere dichiarata responsabile per una pratica che è purtroppo consentita, seppur illegittima;

- la modifica delle modalità di accesso all'internet banking, già programmata anteriormente ai fatti contestati, è stata introdotta al fine di semplificare il processo, così come comunicato ai clienti con specifica comunicazione;
- pertanto, la truffa rientra sostanzialmente in una normale frode di phishing/vishing;
- la diffusione di tali fenomeni è tale che ormai i Collegi Abf ritengono che l'impiego della media diligenza sia sufficiente a scongiurare il pericolo e a impedire la truffa;
- per quanto attiene la presunta anomalia dell'operazione, la stessa non appare anomala né idonea a configurare un rischio frode oggettivo;
- anche la connessione da un diverso indirizzo IP non costituisce indice idoneo a giustificare il blocco automatico dell'operatività della clientela.

Ciò posto, il ricorrente chiede il rimborso della somma di **€ 28.500,00**, *oltre rimborso delle spese legali stragiudiziali in importo come da parametri di legge ed oltre spese di assistenza legale nella presente procedura".*
L'intermediario resistente chiede il rigetto del ricorso.

DIRITTO

L'operazione contestata consiste in un bonifico disposto da *home banking* in data 30.01.2023 per l'importo di € 28.500,00:
L'intermediario ha riferito che il sistema di autenticazione "*prevede per l'accesso, per l'esecuzione di specifiche operazioni dispositive e per la profilatura di utenti secondari (circostanza esclusa per l'utenza in questione), oltre che l'inserimento del codice utente e password in fase di accesso, una chiamata di sicurezza ("Secure Call" ovvero SCA) al Numero Verde dedicato, effettuata con numero visibile dal cellulare associato all'utenza Master. In seguito all'inserimento delle credenziali, per autenticarsi in maniera rafforzata, viene richiesto di effettuare una chiamata identificativa dal numero di cellulare dell'utente al numero verde dedicato e la digitazione dal codice a 4 cifre che compare a video in fase di autenticazione*".
Parte resistente ha specificato che il cliente "*il 30 gennaio 2023 si connette al servizio di internet banking attraverso il canale desktop da un indirizzo IP (176.xxx.xx.xx) corrispondente al gestore X" […] Il Log registra la corretta autenticazione tramite secure call. La sessione, utilizzata per disporre il pagamento di € 28.500,00, termina alle 6:40:30. […] L'utente ha eseguito l'accesso conoscendo le credenziali mnemoniche user e password*".
L'intermediario ha riferito che l'accesso, così come le singole operazioni dispositive, richiedere un doppio fattore di autenticazione, costituito dall'inserimento delle credenziali statiche di accesso (codice utente e password) e dall'utilizzo della Secure Call. Dal file "logSecureCall", all'orario del login (ora 18:21 e 18:23), vi è evidenza di una operatività del sistema di autenticazione, non è meglio specificato dall'intermediario. Gli orari riportati nel file "LogSecureCall", sembrano coerenti con gli orari dei bonifici di cui al file "Op-online-Cedacri".
Il Collegio di Torino (cfr. decisione 117245/2023 e decisione n.559/2024) ha ritenuto provato il sistema di autenticazione dell'intermediario sulla base dei seguenti fattori di autenticazione:
Per l'accesso:

1. elemento di conoscenza: codice utente e password;
2. elemento di possesso: Secure Call al numero verde effettuata tramite numero certificato del cliente, con conseguente inserimento del PIN che compare a video.

Per la singola operazione:

1. elemento di conoscenza: codice utente e password (mutuate dall'accesso);
2. elemento di possesso: Secure Call al numero verde effettuato tramite numero certificato del cliente, con conseguente inserimento del PIN che compare a video.

L'intermediario ha riferito che la Secure Call, che identifica sia nel login che nell'autorizzazione del bonifico il fattore di possesso, sarebbe stata effettuata dal numero certificato del cliente, e tale circostanza sembrerebbe confermata dai log relativi alla Secure Call.

Tuttavia parte ricorrente ha eccepito di non aver mai effettuato la chiamata al numero per la Secure Call e, a supporto, ha allegato i tabulati telefonici, ricevuti dal proprio operatore telefonico, dai quali effettivamente non emergono chiamate verso il numero dell'intermediario, il quale nelle controrepliche sembrerebbe aver ammesso la possibilità che il presidio rappresentato dal numero verde per la Secure Call (che rappresenta l'elemento di possesso) possa essere "aggirato" dai truffatori tramite il meccanismo del *caller id spoofing*, cioè "*simulando di essere l'utente che utilizza la piattaforma della banca*":

È evidente che se è possibile per un truffatore poter eseguire un *spoofing* verso l'intermediario - facendo cioè comparire, nel processo di autorizzazione di Secure Call, come numero chiamante quello del cliente - viene meno il fattore di autenticazione di possesso legato al numero di cellulare dell'utente, secondo un meccanismo del tutto assimilabile a quello della "*sim swap fraud*", nel quale il fattore di possesso (il numero di cellulare del cliente) viene compromesso tramite l'effettiva appropriazione, da parte del malfattore, del numero di cellulare certificato tramite la richiesta di emissione di una nuova SIM da parte dell'operatore telefonico. Nel caso di specie, quindi, il presidio posto dal fattore di possesso viene aggirato tramite il meccanismo dello spoofing verso il numero di Secure Call.

È pacifico l'orientamento dell'Arbitro secondo cui la "*sim swap fraud*" opera non sul versante della colpa grave del cliente, ma su quello dell'autenticazione, rendendo in tal modo insufficiente la prova della SCA offerta da parte dell'intermediario.

È orientamento condiviso dei Collegi, in considerazione, da un lato, del rischio di impresa connesso all'affidamento parziale a terzi soggetti – l'operatore telefonico – della procedura di autenticazione delle operazioni di pagamento (attraverso l'invio dell'OTP con sms su cellulare) e, dall'altro, dell'eventuale emersione anche di fenomeni di *phishing*, ritenere che il ricorso vada accolto integralmente: in tale fattispecie la sostituzione della SIM card deve essere infatti equiparata alla mancanza di autenticazione dell'operazione di pagamento ai sensi e per gli effetti dell'art. 10 del D.lgs. 11/2010.

Deve essere esaminato un ulteriore profilo.

Parte resistente ha eccepito che la parte ricorrente non ha indicato le circostanze di fatto della frode subita.

Secondo gli orientamenti condivisi dei Collegi, a differenza delle ipotesi di furto o smarrimento dello strumento di pagamento, rispetto ai quali la mancata autorizzazione dell'operazione di pagamento sarebbe legalmente presunta, nel caso di contestazioni di utilizzi fraudolenti *on line* di strumenti di pagamento le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo, ma solo qualora:

i) l'intermediario abbia offerto la prova dell'autenticazione delle transazioni disconosciute;
ii) il sistema di pagamento risulti conforme alla *Strong Customer Authentication*;
iii) non risultino indici di anomalia delle operazioni e/o ulteriori elementi.

Nel caso di specie non ricorre il secondo requisito, quindi l'eccezione deve essere disattesa.
L'intermediario ha allegato una schermata per indicare l'invio di notifiche tramite sms e/o email. Tuttavia la posizione condivisa dei Collegi vede come irrilevante la mancata attivazione ovvero il mancato funzionamento del servizio di sms-alert (o di servizio assimilabile) nei casi in cui la ricezione dell'alert non possa in concreto limitare il pregiudizio dell'utente, ossia nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più operazioni a distanza di pochi minuti l'una dall'altra.
L'intermediario non ha richiesto l'applicazione della franchigia, che, secondo gli orientamenti condivisi dei Collegi, non è applicabile in assenza di espressa richiesta dell'intermediario nelle proprie controdeduzioni.
La parte ricorrente ha domandato anche il "*rimborso delle spese legali stragiudiziali in importo come da parametri di legge ed oltre spese di assistenza legale nella presente procedura*". La ricorrente non ha stata depositata la notula dell'avvocato.
Il Collegio di coordinamento n. 3498/2012 ritiene che "*là dove sia dimostrato che la parte ricorrente si sia avvalsa, nell'intero snodo procedimentale che va dal reclamo al ricorso, dell'ausilio di un difensore sopportandone il relativo costo, quest'ultimo possa e debba prendersi in considerazione, in caso di accoglimento del ricorso che si concluda con l'accertamento di un diritto risarcitorio, non già quale autonoma voce di rimborso non prevista dal Reg. ABF, bensì quale componente del più ampio pregiudizio patito dalla parte ricorrente. In tale valutazione, il Collegio giudicante deve naturalmente attenersi a criteri di estrema prudenza, che includono l'accertamento dell'effettivo sostenimento dell'onere defensionale, della sua funzionalità alla gestione del procedimento, della ragionevolezza e coerenza dell'importo richiesto rispetto al valore e alla complessità della controversia, risultando pertanto l'importo di tale componente di pregiudizio stimabile anch'esso in via equitativa*". Come indicato, nel caso l'effettivo sostenimento della spesa non è dimostrato e la domanda non può essere accolta.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 28.500,00.
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
EMANUELE CESARE LUCCHINI GUASTALLA