Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) MINNECI	Membro designato dalla Banca d'Italia
(MI) FERRETTI	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MINNECI UGO

Seduta del 05/10/2021

FATTO

Parte ricorrente riferisce:

- di essere titolare del c/c n. XX96 presso l'intermediario;
- di avere ricevuto alle ore 12:54 dell'11.11.2020 una telefonata da un numero riconducibile apparentemente all'intermediario;
- che l'interlocutore - qualificatosi come un operatore dello stesso - lo informava dell'esistenza di un bonifico sospetto e lo invitava a comunicargli un codice token per annullare la disposizione ed avviare la procedura di blocco;
- che, in buona fede e sicuro della lecita provenienza della telefonata, seguiva le indicazioni del sedicente operatore e comunicava il codice pervenuto via sms;
- che, subito dopo, riceveva un messaggio di avvenuta cancellazione del bonifico che proveniva dal numero telefonico ufficiale dell'intermediario;
- che, quindi, controllava il proprio estratto conto e non rilevava nessun bonifico in uscita;
- che solamente nella giornata successiva, ricontrollando i propri movimenti bancari dalla home banking del portale della banca, constatava che era stata decurtata dal suo conto corrente la somma di € 9.000,00;
- che, in filiale apprendeva di essere stato vittima di vishing e disconosceva l'operazione;

- di essere stato tratto in inganno dalla provenienza della telefonata e del messaggio e che questo tipo di truffa è stata classificata dall'ABF quale "sofisticata" proprio in ragione della riconducibilità a canali ufficiali;
- che l'intermediario non ha adempiuto ai propri obblighi di protezione dei sistemi informatici/dati personali dei clienti, anche alla luce dell'art. 2050 c.c. e della legislazione vigente a tutela della privacy, come confermato anche dalla giurisprudenza di legittimità e da numerose decisioni ABF in tema.

Tutto ciò premesso, domanda la retrocessione della somma fraudolentemente sottratta.

In sede di controdeduzioni, l'intermediario convenuto eccepisce:

- che il cliente è cointestatario del rapporto di corrente n. XX96 acceso presso l'intermediario;
- che il cliente aveva aderito al Servizio di home banking, e aveva altresì attivato il servizio SMS Alert che ha prodotto a fronte di ciascuna delle operazioni contestate il relativo SMS;
- che il servizio di home banking prevede l'accesso alle funzioni di inquiry e dispositive mediante un sistema di autenticazione "forte", in linea con la normativa europea PSD2;
- che l'attivazione del Mobile Token è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'home banking, come effettivamente avvenuto nel caso di specie;
- che il ricorrente dichiara in denuncia e nella successiva integrazione di avere rivelato a terzi codici personali, a lui strettamente riservati, che non avrebbe dovuto comunicare a nessuno;
- che per quanto attiene alla telefonata, proveniente dal n. 06****, è risaputo che il "caller ID" che appare su telefono fisso o mobile non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display;
- che il cliente ha ricevuto sul proprio cellulare il relativo SMS alert che gli confermava l'inserimento dell'operazione, mentre non vi è alcuna dimostrazione, neppure da parte del ricorrente, dell'SMS che secondo quanto si legge in denuncia gli comunicava l'annullamento del bonifico di euro 9.000,00;
- che la frode è stata resa possibile esclusivamente in ragione della colpa grave del ricorrente che ha comunicato ai presunti frodatori l'OTP necessario per l'attivazione del Mobile Token;
- che la diffusione del fenomeno è tale che i Collegi ABF ormai ritengono da tempo che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa;
- che la reticenza nella narrazione dei fatti occorsi viene condannata dall'orientamento diffuso dei Collegi Territoriali ABF;
- che per la salvaguardia della propria clientela dal rischio frode, anche in data 04.08.20 la banca ha promosso un'azione di mailing indirizzata a tutta la clientela (di cui è prodotta evidenza);
- che dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi, le operazioni risultano correttamente autenticate, registrate e contabilizzate (così come previsto dall'art. 10 del D. Lgs. n. 11/2010), come dimostrato nelle evidenze LOG;
- che, a seguito del disconoscimento dell'operazione, la banca ha prontamente verificato il conto corrente del beneficiario ma le somme non erano già più disponibili.

Ciò posto, insiste per il rigetto del ricorso.

Con successive Repliche, le parti ribadiscono le rispettive posizioni.

DIRITTO

Nell'affrontare la presente controversia, occorre preliminarmente sottolineare l'assoggettabilità della stessa alla disciplina di cui al decr. lgs. n. 11/2010 nella versione oggi vigente; risulta infatti contesta una operazione di pagamento dell'importo di Euro 9.000,00, eseguita nel novembre 2020.
Sempre *in limine*, deve segnalarsi che parte ricorrente riferisce di essere rimasta vittima di un episodio di vishing. A tale riguardo, preme fin da subito notare che sussiste prova agli atti della riconducibilità della chiamata ricevuta dal cliente a un canale ufficiale dell'intermediario convenuto. Più nel dettaglio, è dato evincere che al sedicente operatore della banca resistente parte ricorrente abbia comunicato i codici necessari per attivare il mobile token e dare corso all'operatività fraudolenta.
Tutto ciò premesso, mette conto di precisare che, per l'ipotesi di disconoscimento di operazioni da parte del cliente, il suddetto decreto fissa – all'art. 10 – un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione 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; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.
Ora, con riguardo al caso di specie, può considerarsi acquisita la prova richiesta dal comma 1 dell'art. 10, avendo l'intermediario offerto idonea documentazione informatica in ordine alla corretta registrazione, autenticazione e contabilizzazione della operazione contestata.
Più delicata si presenta la questione con riguardo all'elemento della colpa grave.
In effetti, per quanto sia rimasta vittima di un episodio di vishing (la chiamata telefonica apparendo riconducibile a una utenza dell'intermediario) e pertanto di una aggressione informatica sofisticata, la condotta del cliente avente ad oggetto la comunicazione delle credenziali di sicurezza relative all'utilizzo dello strumento di pagamento appare comunque connotata da profili di leggerezza non veniale.
D'altro canto, non può neppure tacersi che dalla vicenda in esame risultano emergere alcune problematicità anche con riguardo alla organizzazione stessa del servizio prestato dall'intermediario convenuto.
Più precisamente, è vero che, sulla base di quanto risulta agli atti, l'intermediario convenuto ha adottato un sistema a doppio fattore di sicurezza (l'operazione contestata risultando essere state autenticata anche attraverso un codice OTP); è però altrettanto vero che il sistema antifrode del medesimo ha gestito una situazione oggettivamente insidiosa, come l'abilitazione su un nuovo device del c.d. mobile token (strumento in grado di generare una password dinamica otp per conferma delle operazioni dispositive mediante App), attraverso una procedura che non appare fornire adeguati standard di

sicurezza, dovendosi all'uopo reputare necessaria l'adozione di misure ulteriori che permettano un effettivo controllo sulla identità e reale volontà del soggetto richiedente l'enrollement (se del caso, prendendo diretto contatto con il cliente o disponendo il blocco cautelativo della operatività).
In tale contesto, l'ampia informativa in materia di sicurezza e prevenzione delle truffe resa disponibile sul proprio sito Internet dalla banca in favore della clientela si presta senz'altro ad integrare una iniziativa apprezzabile; ma non può da sola supplire agli inconvenienti appena riferiti. Quello delle frodi informatiche costituisce infatti un rischio tipico dell'attività di offerta di servizi di pagamento, destinato - come tale – a gravare (almeno in linea di principio) sull'intermediario. E ciò tanto più allorquando la concreta organizzazione del servizio rifletta indici aggiuntivi di pericolosità (se non altro rispetto a clienti che rivestano la qualità di consumatore), come l'attivazione di un tipo di token in grado di generare autonomamente codici otp, così permettendo l'avvio di una operatività suscettibile di svolgersi al di fuori della possibilità del benché minimo controllo da parte del cliente (se non a cose ampiamente fatte attraverso la constatazione degli addebiti sull'estratto conto).
Il vero è che il caso in esame risulta proporre una situazione di concorso di colpa da regolare - anche facendo uso di criteri equitativi - alla luce dell'art. 1227 c.c.
In tale prospettiva, gli elementi richiamati, unitamente alle evidenze probatorie in atti, inducono ad addossare sull'intermediario convenuto la perdita subita dal ricorrente in misura pari alla metà dell'ammontare sottratto. Sarà pertanto da considerare dovuta in favore di parte ricorrente la somma di Euro 4.500,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di Euro 4.500,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00, quale contributo alle spese della procedura, e alla parte ricorrente la somma di Euro 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA