Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) MINNECI

Seduta del 29/04/2021

FATTO

Parte ricorrente propone tre distinti ricorsi premettendo le medesime circostanze di fatto, ovvero:

- di avere ricevuto, in data 18 maggio 2020, segnalazioni da ogni canale ufficiale della Banca convenuta (mail, SMS e chiamate telefoniche) relative a un tentativo di accesso non autorizzato al proprio account bancario;
- di non avervi dato assolutamente seguito;
- di essere stato poi contattato dal numero verde dell'intermediario e di avere, a quel punto, seguito le indicazioni del sedicente operatore dell'intermediario che chiedeva conferma di dati già in suo possesso;
- di avere successivamente scoperto l'avvenuto addebito di operazioni non autorizzate.

Ciò posto, con il primo ricorso disconosce due prelievi cardless, il primo di Euro 1.000,00, l'altro di Euro 2.000,00 e conseguentemente chiede la retrocessione del relativo ammontare.
Con il successivo ricorso, disconosce un bonifico di Euro 1.000,00 e chiede la retrocessione del relativo ammontare.
Con il terzo ricorso, disconosce un pagamento on line di Euro 1.708,99 per acquisto tramite sito e chiede la retrocessione del relativo ammontare.

In sede di controdeduzioni, l'Intermediario convenuto chiede preliminarmente la riunione dei tre ricorsi. Ciò posto, insiste per il rigetto dei stessi, svolgendo le medesime difese.
In particolare, quanto al merito dei fatti, precisa che:

- il Cliente è titolare di un conto corrente abilitato al servizio di *internet banking*;
- in data 18.05.2020, tramite il predetto servizio, venivano disposte due operazioni di prelievo cardless, per un importo complessivo pari a € 3.000,00;
- il servizio di *internet banking* è dotato di sistema di autenticazione forte "a due fattori".

Con specifico riguardo alle modalità di funzionamento del servizio di internet banking, sottolinea:

- di aver adottato modalità di funzionamento con autenticazione "a due fattori", in conformità alle disposizioni del Reg EU 2018/389;
- di richiedere pertanto al Cliente, al momento dell'accesso, di autenticarsi attraverso l'inserimento simultaneo di password statiche (codice Titolare e codice PIN) e di password dinamica OTP (codice O-Key, generato via software dall'APP apposita o inoltrato via SMS al numero di cellulare certificato dal Cliente);
- di richiedere ulteriormente al Cliente, per l'esecuzione di talune operazioni di pagamento, di identificarsi tramite: i) risposta alle domande di sicurezza precedentemente censite; ii) in mancanza di queste, digitazione di un secondo codice di sicurezza inviato via SMS dalla Banca;
- di mettere costantemente a disposizione della Clientela, sul proprio sito Internet, ampia informativa in materia di sicurezza e prevenzione delle truffe.

Rispetto agli obblighi, previsti dalla legge a carico del prestatore di servizi di pagamento, l'Intermediario eccepisce di aver nel caso di specie correttamente adempiuto agli stessi, avendo dato esecuzione alle operazioni contestate a seguito del corretto inserimento di tutte le credenziali possedute dal Cliente. Asserisce infatti;

- di aver rilevato l'accesso al servizio di *internet banking* da un IP diverso da quello abitualmente usato dal Cliente, e di avergli perciò inoltrato:
  a) apposita push di alert;
  b) codice di sicurezza a mezzo SMS;
- di aver eseguito l'enrollment di un nuovo device, solo previa validazione del relativo codice di sicurezza;
- di aver in seguito richiesto ulteriore conferma delle operazioni di prelievo cardless disposte, con apposito codice OTS inviato a mezzo SMS;
- di aver eseguito le operazioni solo a seguito di validazione dei codici OTS.

Ciò posto, richiama l'attenzione su alcune circostanze suscettibili di far ravvisare la colpa grave del Cliente, rilevando come, per sua stessa ammissione, quest'ultimo abbia:

- inserito i propri codici personali a seguito della ricezione di un SMS;
- seguito le indicazioni di un sedicente operatore del numero verde, rispondente in realtà ad utenza non riconducibile a quelle usate dalla Banca;
- dato così seguito ad una truffa non particolarmente sofisticata, non essendo le modalità della stessa assolutamente assimilabili ad alcuna operatività della Banca;

- colpevolmente ignorato le push di alert e gli SMS, a mezzo dei quali la Banca lo informava dell'avvenuto accesso al conto e dell'inserimento dell'operazione contestata.

Domanda pertanto il rigetto delle pretese avversarie di cui ai tre ricorsi proposti.

Nelle successive Repliche, le parti ribadiscono le proprie richieste.

DIRITTO

Nell'affrontare la presente controversia, occorre preliminarmente sottolineare che, relativamente alla vicenda materiale che forma oggetto della presente controversia, parte ricorrente ha proposto nei confronti del medesimo intermediario tre distinti ricorsi diretti ad ottenere la retrocessione dell'ammontare di una pluralità di operazioni di pagamento disconosciute. Anche tenuto conto di quanto richiesto dall'intermediario convenuto, ricorrono ragioni di evidente opportunità per la riunione dei procedimenti, stante l'esigenza di una valutazione unitaria delle modalità realizzative dell'asserita condotta truffaldina.
Sempre in limine preme fin da subito sottolineare l'assoggettabilità della controversia in oggetto stessa alla disciplina di cui al decr. lgs. n. 11/2010 nella versione oggi vigente; risultano infatti contestate quattro operazioni (due prelievi cardless per un importo pari a Euro 3.000,00 tramite il ricorso più antico, un bonifico di Euro 1.000,00 mediante successivo ricorso e un pagamento on line di Euro 1.708,99 attraverso il terzo ed ultimo ricorso), per un ammontare complessivo di Euro 5.708,99, tutte eseguite il 15 maggio 2020.
Sempre *in limine*, deve segnalarsi che parte ricorrente riferisce di essere rimasta vittima di un episodio di spoofing misto a vishing. A tale riguardo, preme fin da subito notare che se sussiste prova agli atti della esistenza di un SMS spoofing ovvero di un SMS "civetta" memorizzato dal cellulare in coda a quelli genuinamente inviati dalla banca, non vi è per contro evidenza (in difetto della allegazione da parte ricorrente dello screenshot del registro chiamate) della provenienza di successive chiamate truffaldine dal numero verde dell'intermediario.
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 delle operazioni contestate.
Più delicata si presenta la questione con riguardo all'elemento della colpa grave.

In effetti, per quanto sia rimasta vittima di un SMS spoofing (il messaggio truffaldino arrivando in coda ai normali sms dell'intermediario) e pertanto di una aggressione informatica sofisticata (lo spoofing consistendo nella manipolazione dei dati relativi al mittente di un messaggio per far sì che esso appaia provenire da un soggetto differente, mediante la sostituzione del numero originario con un testo alfanumerico riconducibile a quello utilizzato dall'intermediario per i propri messaggi genuini), la condotta del cliente appare connotata da profili di leggerezza non veniale sia per avere comunicato le credenziali di sicurezza relative all'utilizzo dello strumento di pagamento, dopo essere stato contattato da una utenza telefonica la cui riconducibilità all'intermediario convenuto non è stata in realtà dimostrata; sia per avere trascurato notifiche push e sms provenienti dalla banca resistente segnalanti l'operazione di enrollment del device.
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 (le operazioni contestate essendo state autenticate anche attraverso un codice OTP); è però altrettanto vero che il sistema antifrode del medesimo ha gestito una situazione oggettivamente insidiosa, come la certificazione di un nuovo device, attraverso una procedura (quella contemplante l'invio di notifiche SMS/push) 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 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'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 la previsione di un massimale giornaliero elevato (in quanto pari a Euro 30.000,00) oppure la possibilità di inoltrare bonifici nella sola modalità istantanea.
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 al 50%.

Sussistono pertanto le condizioni per ritenere la banca resistente tenuta a retrocedere l'importo (arrotondato) di Euro 2.854,00, pari al 50% dell'ammontare complessivo (di Euro 5.708,99) delle operazioni disconosciute.

PER QUESTI MOTIVI

Il Collegio, riuniti i ricorsi, accoglie parzialmente le domande e dispone che l'intermediario corrisponda alla parte ricorrente la somma di Euro 2.854,00.
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