Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Decisione N. 11938 del 26 agosto 2022

**COLLEGIO DI BOLOGNA**

composto dai signori:

| | |
|---|---|
| (BO) MARINARI | Presidente |
| (BO) BERTI ARNOALDI VELI | Membro designato dalla Banca d'Italia |
| (BO) LOMBARDI | Membro designato dalla Banca d'Italia |
| (BO) PASQUARIELLO | Membro di designazione rappresentativa degli intermediari |
| (BO) PETRELLI | Membro di designazione rappresentativa dei clienti |

Relatore PATRIZIA PETRELLI

Seduta del 26/07/2022

**FATTO**

Con ricorso depositato in data 15 aprile 2022 riferisce quanto che: è titolare della carta associata al conto corrente in essere presso l'intermediario; il 6.9.2021 richiedendo il saldo del conto presso un ATM constatava che sul conto vi era una giacenza di pochi centesimi; il giorno successivo, presso la filiale dell'intermediario, emergeva l'esecuzione di 21 movimentazioni di addebito sconosciute e mai autorizzate effettuate tra il 27 agosto 2021 e il 2 settembre 2021 riportanti l'indicazione generica di "pagamento internet" per un totale di 16.206,00 euro; i pagamenti sono stati eseguiti presso un sito internet di scommesse sportive; il ricorrente non ha mai divulgato i codici di sicurezza della carta né li ha mai inseriti in siti web; in ragione delle peculiari caratteristiche dell'attività tecnica di cui si discute e dell'elevata professionalità della resistente, troverà applicazione il disposto dell'art. 2050 c.c. atteso che l'attività bancaria si caratterizza per essere un'attività (intrinsecamente) pericolosa; la resistente è responsabile ai sensi dell'art. 2050 c.c. per il danno derivante al ricorrente dall'illecita sottrazione di somme di denaro dal proprio conto corrente e, pertanto, dovrà essere condannata a risarcire integralmente il danno da questa subito, per l'ammontare complessivo di 16.206,00 euro, oltre interessi e rivalutazione monetaria; in via subordinata, la resistente dovrà essere condannata al risarcimento del danno subito dal ricorrente per aver colpevolmente inadempiuto agli obblighi di cui al D.Lgs. n. 11/2010, alle specifiche pattuizioni contrattuali che regolavano il

rapporto di conto corrente, nonché alle generali regole di condotta di cui agli artt. 1175, 1176, co. 2, 1375 e 1710 c.c.; nel caso di specie, infatti, il processo di autorizzazione nel suo complesso non è stato minimamente rispettato dalla resistente, mancando addirittura il primo dei suoi elementi essenziali: il cliente non ha mai prestato il proprio consenso per i pagamenti per i quali è causa; oltre a non aver mai disposto alcun pagamento, né autorizzato alcuna operazione, non ha mai ricevuto alcun codice o altra misura di strong authentication; né ha mai ricevuto alcun alert o informazione da parte dell'intermediario; risulta chiaro che le misure di sicurezza predisposte dall'intermediario, nel caso di specie, per l'autenticazione del disponente e per l'autorizzazione dei pagamenti disconosciuti sono, alla luce del progresso tecnologico, del tutto insufficienti a garantire l'effettiva tutela del cliente; in via subordinata, la resistente dovrà essere condannata al risarcimento del danno subito dal ricorrente in forza del combinato disposto degli artt. 82 del Regolamento Europeo n. 679 del 27.04.2016 (di seguito anche solo GDPR o il Regolamento) e 2050 c.c.; nel caso di specie, si è visto che il rischio di un accesso illecito da parte di terzi ai conti correnti dei clienti è un evento più che prevedibile e comporta il rischio di un grave e concreto pregiudizio per i diritti del correntista; ciononostante, la resistente ha evidentemente omesso di adottare, riesaminare e comunque aggiornare le misure di sicurezza e di controllo di modo che queste fossero idonee ad impedire l'accesso ai dati sensibili dei propri clienti da parte di terzi; la resistente, quale titolare del trattamento dei dati personali, è responsabile dei danni subiti dal correntista per non aver impedito a terzi di introdursi illecitamente nel sistema telematico mediante la captazione dei suoi codici di accesso e, pertanto, per non aver impedito il compimento delle disposizioni illegittime.

Pertanto si rivolge a questo Arbitro chiedendo il rimborso della somma complessiva pari a 16.206,00 euro corrispondente all'importo delle operazioni disconosciute, oltre interessi, rivalutazione monetaria e le spese per l'assistenza difensiva.

Costituendosi del procedimento l'intermediario evidenzia che: parte ricorrente, titolare di carta, richiede in questa sede il rimborso della somma portata da operazioni di pagamento on line disposte dal 27.8.2021 al 2.9.2021; nella documentazione allegata al reclamo e al successivo ricorso, la cliente non dichiara di aver mai ricevuto e/o risposto a comunicazioni potenzialmente truffaldine volte a carpire le credenziali di accesso ai suoi strumenti di pagamento. Tuttavia, appurare la modalità attraverso cui è avvenuta la captazione dei dati utilizzati per effettuare le transazioni oggetto della presente contesa, si delinea come elemento determinante per accertare eventuali responsabilità derivanti da una condotta negligente del titolare dello strumento di pagamento; proprio l'assenza di un qualsiasi cenno ad una qualsivoglia operatività online intrapresa in concomitanza dell'illecito addebito, porta a desumere che la presente frode sia riconducibile alla tipologia di phishing definita "classica" nella Decisione del Collegio di Coordinamento 3498/2012; dunque il cliente avrebbe contribuito in maniera determinante alla compromissione del suo dispositivo di pagamento, fornendo incautamente a terzi i dati che invece era tenuto a custodire; le operazioni di pagamento disconosciute risultano regolarmente autorizzate al primo tentativo e senza essere stata precedute da richieste negate; le transazioni disconosciute hanno comportato l'impiego del cosiddetto "sistema di autenticazione a due fattori", il "3DS" che tuttora rappresenta la tecnologia reputata più avanzata ed affidabile nell'ambito dei pagamenti online; con riferimento particolare alle tre transazioni da euro 5,00 eseguite con modalità "no sca" si osserva che, come previsto dalla normativa psd2 (regolamento delegato (ue) 2018/389 della Commissione del 27 novembre 2017, art. 16), per importi che non superino gli euro 30,00 ed al verificarsi delle condizioni previste dal medesimo articolo, è prevista l'operatività on line in 3ds senza necessità di autenticazione forte da parte del cliente, pur rimanendo le transazioni

securizzate; parte ricorrente avrebbe potuto evitare la truffa utilizzando la diligenza media, posto che l'intermediario interloquisce con i propri clienti solo tramite canali ufficiali e mai richiedendo la comunicazione di dati relativi agli strumenti di pagamento forniti.

Pertanto conclude chiedendo il rigetto del ricorso.

In sede di repliche parte ricorrente contesta integralmente le controdeduzioni dell'intermediario e precisa quanto segue: non ha mai comunicato a terzi le sue credenziali di accesso al servizio fornito dalla resistente. Né ha mai ricevuto messaggi fraudolenti volti a carpirgliele; ciò non esclude che terzi, impossessatisi o scoperte le password, abbiano potuto disporre illecitamente delle somme depositate nel conto corrente in assenza di prova concreta di particolari sistemi di allerta o di blocco delle operazioni; la resistente non è stata in grado di giustificare quanto accaduto; la responsabilità dell'intermediario per operazioni effettuate a mezzo di strumenti elettronici, con particolare riguardo alla verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, ha chiara natura contrattuale; va richiamata la regola generale contemplata dall'art. 1218 c.c. in tema di onere della prova; l'intermediario non ha saputo provare la colpa grave del cliente; secondo l'orientamento consolidato della giurisprudenza di legittimità, da ultimo ribadito dalla recentissima ordinanza Cass. 16417/2022 in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema, è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo.

**DIRITTO**

Le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

A fronte del disconoscimento delle operazioni di pagamento da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi dell'art. 10, comma 1, del D. lgs. 11/2010, che così statuisce: "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, 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".

Con riguardo alla modalità di autenticazione delle operazioni, l'art. 10-*bis* del medesimo D. lgs. n. 11/2010 prevede: "Conformemente all'articolo 98 della direttiva (UE) 2015/2366

e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

L'art. 1, lettera q-*bis* del medesimo decreto chiarisce, conformemente alla suddetta direttiva, che la c.d. autenticazione forte consiste in "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

Sul punto, è intervenuta l'EBA con la "Opinion" del 21 giugno 2019 (richiamata espressamente dal Regolamento UE/2018/389 del 27/11/2017) con cui ha precisato, ai fini dell'implementazione del suddetto Regolamento, quali elementi costituiscano o meno, allo stato attuale della tecnologia, fattori di autenticazione forte all'interno delle categorie della conoscenza, del possesso e dell'inerenza.

Così brevemente riassunto il quadro normativo, occorre verificare se nella specie l'intermediario abbia fornito elementi in sostegno della legittimità delle operazioni contestate.

La ricorrente disconosce ventuno operazioni di pagamento *on line* di cui cinque eseguite in data 27/08/2021 tra le ore 23,15 e le ore 23,46; quattro eseguite in data 28/08/2021 tra le ore 00,03 e le ore 00,06; quattro eseguite in data 29/08/2021 tra le ore 00,00 e le ore 00,05; cinque eseguite in data 01/09/2021 tra le ore 00,00 e le ore 00,04 e tre eseguite in data 02/09/2021 tra le ore 00,06 e le ore 00,09 per un importo complessivo pari a 16.206,00 euro, corrispondente a quanto richiesto in restituzione.

Nel caso di specie la documentazione fornita dall'intermediario non consente di ritenere sufficientemente protettivi per il cliente i presidi di sicurezza predisposti, in quanto non risulta che le operazioni contestate siano state autenticate mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. "autenticazione forte".

L'intermediario, al riguardo, afferma che le operazioni disconosciute risultano regolarmente autorizzate al primo tentativo (vedi "spunta verde") e senza essere state precedute da richieste negate (eventualmente contrassegnate da una "X" rossa).

A sostegno produce evidenza relativa alla registrazione della carta intestata alla controparte al protocollo di sicurezza 3D e le relative richieste della SCA.

Null'altro viene prodotto; in particolare non risulta prodotta la documentazione attestante l'invio dei messaggi recanti i codici OTP.

Con riferimento particolare alle tre transazioni da 5,00 euro l'intermediario osserva che, come previsto dalla normativa PSD2 (REGOLAMENTO DELEGATO (UE) 2018/389 DELLA COMMISSIONE del 27 novembre 2017, art. 16), per importi che non superino gli euro 30,00 ed al verificarsi delle condizioni previste dal medesimo articolo, è prevista l'operatività on line in 3ds senza necessità di autenticazione forte da parte del cliente, pur rimanendo le transazioni securizzate.

Sul punto il Collegio ricorda che, in base alle Q&A 2018-4042 dell'EBA, qualora l'intermediario decida di non adottare l'autenticazione forte, applicando un'esenzione alla SCA normativamente prevista (come nel caso di specie), resta ferma la sua

responsabilità, qualora le operazioni siano state disconosciute dal cliente.

Pertanto nello specifico, l'intermediario, al fine di dimostrare la corretta autenticazione delle operazioni e l'assenza di anomalie, non ha fornito evidenze informatiche o contabili certe che, nel caso concreto, simili presidi di sicurezza, conformi ai parametri SCA, siano stati applicati all'operazione disconosciuta.

Secondo l'orientamento dei Collegi ABF (v. *ex multis* Collegio di Bologna, decisione n. 597/2022 e n. 18571/2021), l'intermediario deve fornire la prova di aver adottato una procedura di autenticazione forte tanto nella fase di accesso all'*home banking* quanto nel momento dell'esecuzione delle operazioni.

Tanto premesso, il Collegio ritiene che, nel caso di specie, l'intermediario non abbia fornito la prova della regolarità formale dell'operazione, sotto il profilo della "autenticazione forte del cliente", ai sensi della richiamata disciplina.

Al riguardo, mette conto evidenziare la "Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2" del 21/06/2019, nella quale l'Autorità Bancaria Europea ha preso in considerazione specifici esempi di soluzioni tecniche e chiarito quali elementi possono considerarsi conformi a ciascuna delle tre categorie (inerenza, possesso e conoscenza), che rilevano ai fini della sussistenza di una autenticazione forte.

In base al quadro normativo sopra delineato, così come corredato dagli interventi dell'EBA, non può che confermarsi che spetta all'intermediario la prova dell'intervenuta autenticazione forte delle operazioni di pagamento.

In merito alla prova della corretta autenticazione ed esecuzione delle operazioni di pagamento si osserva che i Collegi territoriali ABF hanno condiviso l'orientamento per cui nel caso in cui l'intermediario non abbia assolto all'onere probatorio sull'autenticazione delle operazioni di pagamento contestate dal cliente, di cui all'art. 10, comma 1 del D.lgs. 11/2010, [...] il ricorso venga accolto, posto che la mancanza anche parziale della prova di autenticazione è risolutiva 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 della colpa grave dell'utente.

Secondo l'orientamento consolidato dei Collegi ABF in caso di mancata produzione di documentazione idonea a dimostrare la corretta e regolare autenticazione della transazione contestata, l'intermediario è tenuto al rimborso integrale delle somme, senza applicazione della franchigia (cfr. Collegio di Milano, decisione n. 20530/20; Collegio di Bologna n. 18713/21; Collegio di Torino n. 3464/2018).

Occorre, peraltro, rilevare che, nel caso di specie, risulta integrato uno degli indicatori di anomalia richiamati all'art. 8 del D.M. n. 112 del 30 aprile 2007.

L'art. 8 (Rischio di frode) del D.M. 30.04.2007, n. 112 (Regolamento di attuazione della l. n. 166/2005, sulla "*Istituzione di un sistema di prevenzione delle frodi di pagamento*") prevede che:

*"Si configura il rischio di frode di cui all'articolo 3, comma 1 della legge, quando viene raggiunto uno dei seguenti parametri*

*a) con riferimento ai punti vendita di cui all'articolo 7, lettera b):*

*1. cinque o più richieste di autorizzazione con carte diverse, rifiutate nelle 24 ore, presso un medesimo punto vendita;*

*2. tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita;*

*3. richiesta di autorizzazione, approvata o rifiutata, che superi del 150% l'importo medio delle operazioni effettuate con carte di pagamento, nei tre mesi precedenti, presso il medesimo punto di vendita;*

*b) riguardo alle carte di pagamento sottoposte a monitoraggio di cui all'articolo 7, lettera c):*

*1. sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento;*

*2. una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del plafond della carta di pagamento;*

*3. due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti."*

Le operazioni contestate riportano come causale "*pagamento internet".* Parte ricorrente riferisce che dalle verifiche effettuate si tratterebbe di pagamenti effettuati a favore di un sito di scommesse sportive e tale circostanza non è contestata dall'intermediario.

Con riferimento al parametro di cui alla lett. a) n. 2, risulta che in data 27/08/2021 sono state eseguite 5 operazioni presso lo stesso punto vendita; che in data 28/08/2021 sono state eseguite 4 operazioni presso lo stesso punto vendita; in data 29/08/2021 sono state eseguite 4 operazioni presso lo stesso punto vendita; in data 01/09/2021 sono state eseguite 5 operazioni presso lo stesso punto vendita e in data 02/09/2021 sono state eseguite 3 operazioni presso lo stesso punto vendita; in presenza di tali circostanze, quindi, l'intermediario avrebbe dovuto quantomeno attivarsi presso la ricorrente per verificare l'autenticità delle operazioni.

Alla luce di tali considerazioni, che assorbono, altresì, ogni valutazione sul contegno della ricorrente nella dinamica della frode, merita accoglimento la domanda proposta con conseguente diritto alla restituzione della somma complessiva di 16.206,00 euro.

All'accoglimento del ricorso nei termini sopra indicati consegue la corresponsione degli interessi legali dalla data del reclamo al saldo (cfr. decisione ABF, Collegio di coordinamento n. 5304/2013).

Non può invece essere accolta la richiesta di rivalutazione monetaria sulle somme da restituire, poiché le stesse costituiscono un debito di valuta.

Né, infine, può trovare accoglimento la domanda di rifusione delle spese di assistenza tecnica in ragione del fatto che queste non costituiscono un pregiudizio suscettibile di essere ristorato, considerata la natura non complessa del ricorso *de quo* (v. Collegio di Coordinamento, decisioni nn. 3498/2012 e 6174/2016).

**PER QUESTI MOTIVI**

**Il Collegio – in parziale accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 16.206,00 (sedicimiladuecentosei/00), oltre interessi legali dalla data del reclamo.**

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Decisione N. 11938 del 26 agosto 2022

**Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE

Firmato digitalmente da
MARCELLO MARINARI