Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) [redacted]	Presidente
(BO) [redacted]	Membro designato dalla Banca d'Italia
(BO) [redacted]	Membro designato dalla Banca d'Italia
(BO) [redacted]	Membro di designazione rappresentativa degli intermediari
(BO) [redacted]	Membro di designazione rappresentativa dei clienti

Relatore [redacted]

Seduta del 25/02/2021

Esame del ricorso n. 1047525/2020 del 10/08/2020

proposto da [redacted]

nei confronti di [redacted]

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) [redacted] Presidente

(BO) [redacted] Membro designato dalla Banca d'Italia

(BO) [redacted] Membro designato dalla Banca d'Italia

(BO) [redacted] Membro di designazione rappresentativa degli intermediari

(BO) [redacted] Membro di designazione rappresentativa dei clienti

Relatore [redacted]

Seduta del 25/02/2021

FATTO

Il ricorrente, nella denuncia acclusa al ricorso, deduce:

- di essere titolare di una carta di credito rilasciata dall'intermediario resistente;

- di essere stato, in data 5.5.2020, vittima di una truffa telefonica da parte di ignoti che si palesavano come operatori dell'intermediario e che, con artifici e raggiri, lo inducevano a comunicare informazioni riservate, in quanto preso alla sprovvista ed ignaro delle reali intenzioni dell'interlocutore;

- che, secondo quanto rappresentato al telefono, i dati richiesti servivano a bloccare un fantomatico tentativo di prelievo non autorizzato dalla carta di pagamento, mentre in realtà si perfezionava un reato in suo danno.

Su queste premesse, il ricorrente chiede *"il rimborso … della somma di 1.200,00 euro, fraudolentemente sottratta …"*.

L'intermediario resistente ha depositato le proprie controdeduzioni, chiedendo il rigetto della domanda della parte ricorrente, eccependo:

- che, con reclamo del 7.5.2020, il ricorrente disconosceva un'operazione di pagamento effettuata in data 5.5.2020 per 1.200,00 euro a mezzo della propria carta di credito;

- che il cliente precisava che, in data 5.5.2020 alle ore 18:13, riceveva una chiamata da un presunto operatore della banca, il quale gli comunicava che erano stati effettuati vari

tentativi di acquisto sulla sua carta di credito e che, per procedere allo storno degli addebiti, era necessario comunicargli il codice contenuto in un SMS che avrebbe ricevuto sul suo telefono;

- di avere inserito dei messaggi di prevenzione delle attività fraudolente sia negli estratti conto inviati al ricorrente, sia sui portali e sugli ATM, e che i messaggi contengono l'indicazione precisa che la banca non chiede mai, con alcun mezzo, di fornire i codici di sicurezza ricevuti sul proprio cellulare;

- che il caso di specie va valutato alla stregua di quanto previsto dall'art. 10 del d.lgs. n. 11/2010, il quale enuncia testualmente che, "*qualora l'utente di servizi di pagamento neghi di avere 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";*

- che, nel caso di specie, la transazione disconosciuta dal ricorrente è stata effettuata tramite *internet* ed autenticata mediante l'invio di OTP ("*One Time Password*") sul numero di cellulare fornito dal cliente alla banca e confermato dal medesimo in sede di verbale di denuncia, come dimostra il *log* autorizzazioni;

- che appare evidente, dunque, che il ricorrente abbia operato "*con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti*", come precisato in tema di gravità della colpa dalla Corte di Cassazione, con la sentenza n. 14456/2001.

DIRITTO

I Collegi ABF hanno più volte affermato che nelle controversie relative all'utilizzo fraudolento di strumenti di pagamento occorre valutare, da un lato, la condotta del cliente con riguardo agli obblighi di diligenza nella custodia dello strumento di pagamento e dei dispositivi collegati e, dall'altro, la condotta dell'intermediario, il quale è chiamato ad adempiere al mandato secondo la diligenza professionale e qualificata prevista all'art. 1176 co. 2 c.c.; circostanze, queste, da valutare caso per caso.

Per consolidato orientamento dei Collegi ABF, a fronte del disconoscimento di operazioni di pagamento da parte dell'utente, è onere dell'intermediario provare che le operazioni siano state autenticate, correttamente registrate e contabilizzate, ai sensi dell'art. 10 del d.lgs. n. 11/2010. In mancanza di tale prova, l'intermediario sopporta integralmente le conseguenze delle operazioni disconosciute.

Infatti, la norma richiamata codifica l'inversione dell'onere della prova: *«1. 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. 2. Quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi*

abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7».

L'esigenza di sistemi di autenticazione multifattoriali è normativamente prevista dall'art. 12 co. 2 *bis* del d.lgs. citato, come modificato in seguito all'entrata in vigore del d.lgs. n. 218/2017 (applicabile al caso di specie, essendo entrato in vigore in data 13.1.2018), che ha dato attuazione nel nostro ordinamento alla Direttiva n. 2015/2366/UE del Parlamento Europeo e del Consiglio del 25.11.2015 (cd. PSD2 - *Payment Services Directive 2*) e al Regolamento UE n. 751/2015 del Parlamento Europeo e del Consiglio del 29.4.2015 (cd. IFR - *Interchange Fees Regulation*). La norma prescrive che, "*salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente*", avendo quindi espressamente introdotto l'obbligo per il prestatore di servizi di pagamento di adottare misure di autenticazione forte, prevedendo, al contempo, che il pagatore non sopporti alcuna perdita se il prestatore non esige un'autenticazione forte del cliente.

L'intermediario, a sostegno delle proprie eccezioni, afferma che l'operazione contestata è stata disposta mediante un sistema di autenticazione forte a due fattori. L'accesso ai servizi *online* richiede infatti l'inserimento, prima, del codice titolare e del codice PIN (*password* statiche) e, successivamente, del codice OTP (*password* dinamica) che consente di validare una specifica transazione.

Ciò detto, la decisione del Collegio di Coordinamento ABF n. 22745/2019 ha fissato il seguente principio: "*la previsione di cui all'art. 10 co. 2 del d.lgs. n. 11/2010 in ordine all'onere posto a carico del prestatore dei servizi di pagamento della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente* [anche] *a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente*".

L'intermediario eccepisce che l'operazione contestata risulta regolarmente eseguita, in assenza di anomalie, ed ha prodotto le seguenti evidenze: a) tracciatura dei movimenti della carta corredata da *legenda* esplicativa, dalla quale emerge che l'operazione è stata [redacted] *internet* [redacted] attraverso inserimento dei dati statici della carta [redacted] ("[redacted]"); risulta altresì che non sia stato richiesto un codice PIN [redacted]; b) SMS inviati al ricorrente; C) lista movimenti contenente l'addebito; d) avviso attraverso il quale l'intermediario ha informato i propri clienti circa la diffusione del fenomeno di *phishing*.

La modalità di autenticazione consistente nell'inserimento dei dati statici della carta e del codice OTP dinamico, in passato, è stata ritenuta dai Collegi ABF conforme alle prescrizioni normative in materia di SCA (*Strong Customer Authentication*). Tuttavia, l'Autorità Bancaria Europea (E.B.A.) il 21.6.2019 ha pubblicato una *Opinion* che nega la validità di un simile sistema, in particolare affermando che i dati statici della carta di pagamento (quali PAN, CVV) non costituiscono elementi idonei ai fini della SCA. Secondo il nuovo orientamento, entrato in vigore il 14.9.2019, i dettagli stampati sulla carta di pagamento non costituiscono né un elemento di possesso, né un elemento di conoscenza, ai fini della SCA. Quindi, sebbene la modalità di autenticazione applicata nella fattispecie sia stata, in passato, ritenuta dai Collegi ABF conforme alle prescrizioni normative in materia di SCA, oggi l'autenticazione avvenuta sui dati statici della carta, seppure incautamente forniti dall'utilizzatore al truffatore, non può essere più considerata una

procedura sicura di autorizzazione dell'operazione, in mancanza di ulteriori elementi di carattere dinamico: questo è peraltro l'orientamento emergente a livello di interpretazione e di applicazione resa dai Collegi territoriali di questo Arbitro, nei tempi più recenti (cfr. le decisioni di questo Collegio n. 22586/2020, del Collegio di Roma n. 11271/2020 e 8493/2020 e del Collegio di Napoli n. 17207/2020).

Nella fattispecie, non potendo contare – ai fini della ricorrenza dei requisiti di SCA – sui dati statici della carta, va rilevata la mancanza di un secondo elemento dinamico, diverso e ulteriore rispetto all'OTP inviato alla parte ricorrente, che, combinato con il primo, consentirebbe di ritenere correttamente adottate modalità sicure di autenticazione forte.

In assenza dei due elementi dinamici come sopra richiesti, non può quindi concludersi per l'adozione, da parte dell'intermediario, di un sistema adeguatamente protetto di autenticazione, con conseguente declaratoria della sussistenza di colpa grave in capo a quest'ultimo, con effetto di accoglimento del ricorso, avendo la circostanza rilievo assorbente e decisivo rispetto al comportamento colposo del cliente, che pure ha omesso di adottare tutte le cautele necessarie ai fini della custodia dei codici di accesso e dei dispositivi connessi.

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 1.200,00 (milleduecento/00).

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