



## COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) BARGELLI

Seduta del 10/11/2022

### FATTO

Il cliente afferma di avere ricevuto un *link* in data 22/12/2021 e di averlo aperto per errore, causando il blocco del cellulare. Afferma che i truffatori avrebbero in tal modo avuto la possibilità di prelevare dal suo conto corrente € 12.500,00. Nega di aver fornito codici di accesso, *password* o autorizzazioni di alcun tipo. Chiede il riaccredito di € 12.500,00.

L'intermediario eccepisce la legittima esecuzione e sostanziale regolarità del bonifico *online* contestato in quanto il cliente risulta essersi correttamente autenticato sulla piattaforma *app* con le proprie credenziali ed aver autorizzato l'operazione inserendo il codice di sicurezza al ricevimento della notifica *push*. Dichiarò, inoltre, che, nonostante il cliente dichiarò di non aver ricevuto o risposto a comunicazioni potenzialmente truffaldine, l'assenza di un qualsiasi cenno ad una operatività *online* dallo stesso intrapresa in concomitanza dell'illecito addebito fa presumere che si tratti di una tipologia di *phishing* "classica"; sarebbe dunque improbabile, secondo l'intermediario, che il cliente sia stato vittima di *SIM swap* in quanto non ha lamentato alcuna variazione di intestazione della SIM, la quale ha continuato funzionare anche dopo il riavvio del cellulare. Afferma di aver messo a disposizione del cliente l'attivazione gratuita del servizio di SMS *alert*, servizio attivo di *default* all'interno dell'*app*, di aver tentato il richiamo del bonifico senza successo e di aver reso edotta la propria clientela in merito alle varie forme di *phishing* in uso. Conclude per il rigetto del ricorso.



Il cliente replica di utilizzare la carta di debito per effettuare pagamenti di *routine*, autorizzati tramite codice OTP e di aver subito un attacco di *hacker*; precisa che i truffatori hanno disposto un pagamento di gran lunga superiore rispetto alle spese normalmente sostenute dallo stesso.

L'intermediario controreplica precisando che la procedura di *chargeback* non ha avuto esito positivo a causa del riscontro negativo del beneficiario.

## DIRITTO

Il presente ricorso ha a oggetto un'operazione di bonifico *online* dell'importo complessivo di € 12.500,00, eseguita il 21/12/2021, alle ore 21:07. Sono in atti il modulo di disconoscimento e la denuncia del cliente – presentata il 22/12/2021 – nella quale il cliente afferma di avere aperto il *link* che aveva ricevuto sul proprio cellulare, di avere determinato così il blocco del telefono, non riuscendo a utilizzare le applicazioni installate sullo stesso.

Il Collegio, richiamati, in particolare, gli artt. 10 e 12 del D.lgs. 27 gennaio 2010, n. 11, ricorda che è l'intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione. L'assolvimento di tale onere probatorio, peraltro, non fa presumere la frode del cliente o il mancato adempimento, da parte sua, a uno o più degli obblighi di cui all'art. 7, con dolo o colpa grave (v., *amplius*, Collegio di coordinamento, decisione n. 22745/2019). È, infatti, sempre l'intermediario a dover provare le circostanze capaci di dimostrare le ipotesi nelle quali l'utilizzatore può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. In particolare, la valutazione della condotta dell'utilizzatore dello strumento di pagamento, ai fini dell'eventuale giudizio di dolo o colpa grave, deve fondarsi sulla considerazione del complesso di circostanze che caratterizzano il caso concreto.

Trattandosi di pagamento elettronico, il Collegio deve ulteriormente verificare il sistema predisposto dall'intermediario alla luce dei criteri previsti per l'autenticazione forte e, a tal fine, richiama l'art. 10-*bis* (Autenticazione e misure di sicurezza) e l'art. 12 del d.lgs. 27.1.2010, n. 11 ("Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento"), che recita: "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". Il Collegio ricorda altresì che, in base all'art. 1, lett. q-*bis*, l'"autenticazione forte del cliente" è definita come "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".

I requisiti appena citati – si precisa – devono sussistere sia nella fase di accesso al conto, sia in quella dell'esecuzione delle singole operazioni.

Nel caso di specie, l'intermediario afferma che le operazioni sono state correttamente contabilizzate, registrate e autenticate e ne ricostruisce i singoli passaggi esecutivi. Dichiarà, in particolare, che ai fini dell'accesso al conto sarebbe richiesta la preventiva installazione dell'*app* sul *device*, nonché l'associazione dello strumento di pagamento (carta di pagamento o conto corrente) e la configurazione del codice "P\*\*\*\*\*D" (tramite inserimento delle credenziali di accesso, dei dati dello strumento di pagamento, della *password* dinamica "usa e getta"), ma non produce evidenze atte a supportare tale ricostruzione.



Arbitro Bancario Finanziario  
Risoluzione Stragiudiziale Controversie

L'intermediario, inoltre, riferisce che il bonifico è stato autenticato attraverso l'inserimento del codice di sicurezza "P\*\*\*\*\*D" e produce il dettaglio dei movimenti, ma tale documento non prova l'autenticazione tramite tale codice, né tale tipo di autenticazione è in alcun modo desumibile dall'ulteriore evidenza allegata, che dimostra solo l'avvenuta esecuzione dell'operazione dall'*app*.

Sulla base degli elementi appena esposti, il Collegio conclude che la documentazione prodotta dall'intermediario non sia sufficiente a offrire la prova dell'adozione di un sistema di autenticazione forte, richiesto per i pagamenti elettronici dalle fonti normative su richiamate.

Dato il fallimento della prova dell'adozione di un sistema di autenticazione forte, diviene irrilevante accertare se siano fondate le controdeduzioni dell'intermediario tese a dimostrare la colpa grave del cliente (che sarebbe stato vittima di un tipo di frode facilmente evitabile con una diligenza media) nell'adempimento degli obblighi di cui all'art. 7 del d.lgs. 27.1.2010, n. 11. Per escludere la responsabilità dell'intermediario, infatti, sarebbe necessario provare che il cliente ha agito in modo fraudolento (art. 12 2-*bis* del citato decreto legislativo).

Pertanto, sempre richiamato l'art. 12 2-*bis* del d.lgs. 27.1.2010, n. 11 ("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. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente"), la responsabilità per l'esecuzione fraudolenta del bonifico grava sull'intermediario.

La domanda del cliente, dunque, merita pieno accoglimento.

### **PER QUESTI MOTIVI**

**Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 12.500,00.**

**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

FLAVIO LAPERTOSA