COLLEGIO DI MILANO - DEC. N. 9425/2019 - PRES. LAPERTOSA - REL. AFFERNI

Strumenti di pagamento – onere della prova (d. lgs. n. 11/2010, art. 10)

Grava sull'intermediario l'onere di provare non solo l'insussistenza di malfunzionamenti e la corretta autenticazione dell'operazione ma anche i fatti idonei ad integrare la colpa grave dell'utilizzatore. (IM*CS*).

FATTO

Il cliente – titolare di conto corrente acceso, unitamente alla moglie cointestataria del presente ricorso, presso l'intermediario - si avvedeva che in data 15/06/2017 era stato eseguito dal proprio conto online un bonifico non autorizzato di € 2.850,00.
Detto bonifico risultava eseguito in favore di terzi ignoti.
Sul punto, nella denuncia il cliente rammenta che nella stessa data dell'operazione disconosciuta aveva effettuato una ricarica telefonica mediante il sito dell'intermediario e gli era apparsa una maschera che "chiedeva di inserire i dati della carta con relativo pin, al fine di effettuare degli aggiornamenti". Il cliente aveva ottemperato a tale richiesta.
Dopo la scoperta dell'operazione non autorizzata, il cliente bloccava la propria carta collegata al conto e quella della moglie. Successivamente, scopriva che l'11/05/2017 (e, quindi, oltre un mese innanzi rispetto alla prima operazione fraudolenta scoperta) era stata già compiuta un'altra operazione non autorizzata per l'importo di € 200,00.
Tanto rappresentato, il cliente, unitamente alla moglie, reputa l'intermediario responsabile dell'accaduto e si rivolge all'Arbitro per chiedere la restituzione dell'importo delle operazioni non autorizzate per complessivi € 3.050,00.
Nelle controdeduzioni l'intermediario fa presente che – dalla ricostruzione della vicenda – si evince che i due bonifici sono stati disposti con una distanza di un mese l'uno dall'altro, facendo presumere che gli stessi possano essere stati disposti dal titolare del conto o comunque che il cliente avrebbe dovuto denunciare in un congruo termine tali disposizioni di pagamento.
In alternativa, ritiene che potrebbe trattarsi di un caso di phishing tradizionale di cui il cliente sarebbe rimasto vittima, ponendo in essere una condotta caratterizzata da colpa grave (richiama, sul punto, la decisione n. 3498/2012 del Collegio di Coordinamento e l'art. 1227 c.c.). Ritiene invero che, "Anche se non esplicitato nelle dichiarazioni fornite, sulla base dell'analisi dei dati di fatto, risulta invece assai più plausibile l'ipotesi che la ricorrente abbia abboccato ad un caso di phishing tradizionale ed abbia risposto ad una comunicazione truffaldina ricevuta via email, telefono o SMS". Dalle verifiche effettuate in relazione alla modalità di esecuzione del pagamento è emerso che le transazioni in contestazione sono state eseguite con l'ausilio della tecnologia attualmente reputata più sicura, in quanto, dopo essere state predisposte dal sito dell'intermediario in post-login (ossia a seguito di accesso all'ambiente di pagamento tramite le credenziali statiche dell'utente), le transazioni sono state autorizzate tramite una password monouso che si è generata sul display di un apposito lettore (il cosiddetto PCR, ossia personal card reader) dopo che il correntista ha eseguito un'autenticazione "chip & PIN", e dunque necessariamente con la lettura fisica della carta di pagamento originale collegata al conto e con l'inserimento del relativo codice segreto.
(…)

DIRITTO

Molti dei tentativi di truffa posti in essere con modalità telematiche in materia di servizi di pagamento si svolgono secondo uno schema tipico e ampiamente noto, consistente

nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, sms o altri strumenti di comunicazione, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza (c.d. phishing che, se tradizionalmente prende le forme di una mail civetta, può tuttavia presentarsi anche mediante l'invio di sms – c.d. sms shing – o l'effettuazione di chiamate vocali – c.d. pishing).
La diffusione del fenomeno è tale che i Collegi ABF ormai ritengono da tempo, da un lato, che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa.
La vicenda che ci occupa riguarda un fenomeno di phishing (come dichiarato dalla stessa parte ricorrente nella denuncia ai Carabinieri, ove si legge: "…appariva sullo schermo una maschera che mi chiedeva di inserire i dati della carta con relativo pin, al fine di effettuare degli aggiornamenti ed ovviamente inserivo i dati richiesti").
Al fine di risolvere odierna controversia è dunque necessario analizzare il comportamento dell'intermediario e quello del ricorrente.
Quanto al primo profilo, peraltro assorbente, risulta che l'intermediario resistente non ha prodotto documentazione attestante l'autenticazione, registrazione e contabilizzazione dell'operazione disconosciuta. Sul piano probatorio, è costante l'orientamento di questo Arbitro secondo il quale sull'utilizzatore incombe l'onere della sola allegazione dell'operazione contestata, mentre per l'intermediario detto onere può dirsi adempiuto soltanto qualora costui abbia prodotto in giudizio una documentazione sufficientemente esaustiva e intelligibile attestante la corretta operatività del sistema di pagamento.
Nel caso di specie, si deve altresì considerare che la documentazione allegata dall'intermediario non risulta leggibile, né è stata integrata a seguito di specifica richiesta in fase di sospensione del procedimento. Da tale circostanza non può che derivare l'accoglimento del ricorso. In proposito si richiama l'orientamento consolidato di questo Collegio secondo cui: *"I principi che regolano la materia sono ormai noti e sono quelli fissati dalle disposizioni del D. Lgs. 27.1.2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e dal relativo Provvedimento attuativo della Banca d'Italia del 5.7.2011, applicabili al caso di specie. Alla luce di tali disposizioni, come applicate da questo Arbitro, due sono i passaggi ineludibili in materia. In primo luogo è l'intermediario a dover provare, oltre alla insussistenza di malfunzionamenti, autenticazione, corretta registrazione e contabilizzazione, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento" Collegio di Milano, decisione n. 1588/2017 (si veda anche la più recente decisione del Collegio di Milano, n. 577/19 del 10/01/2019)".*

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 3.050,00 (. ..omissis…)