Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) SANTAGATA DE CASTRO	Membro designato dalla Banca d'Italia
(NA) BOCCHINI	Membro designato dalla Banca d'Italia
(NA) ROSAPEPE	Membro di designazione rappresentativa degli intermediari
(NA) SBORDONE	Membro di designazione rappresentativa dei clienti

Relatore ROBERTO BOCCHINI

Seduta del 08/05/2019

FATTO

Il caso sottoposto all'attenzione di questo Collegio ha ad oggetto il disconoscimento da parte del ricorrente di un bonifico disposto tramite *home banking* per un importo totale di € 3.156,58, eseguito in data 30/07/2018. Provvedeva pertanto a sporgere denuncia alle autorità competenti in data 01/08/2018. Il ricorrente disconosceva formalmente l'operazione, richiedendone l'integrale rimborso, all'esito della fase del reclamo, inutilmente esperita, rispetto alle proprie pretese, adiva l'Arbitro Bancario e Finanziario al fine di veder riconosciuto l'integrale rimborso della somma.
Costituitosi ritualmente, l'intermediario convenuto eccepisce che:

- la ricorrente era stata, presumibilmente, vittima di una truffa telematica,
- l'operazione si era realizzata con l'inserimento delle credenziali di accesso (codice titolare e PIN) ed era stata confermata con l'inserimento del codice OTP generato dal token "O-key", tutti nell'esclusiva disponibilità della ricorrente,
- che dalla tracciatura dell'operazione disconosciuta, era stato possibile verificare che, ritenendo sospetta la transazione, il sistema antifrode in dotazione al servizio di internet banking aveva, altresì, inoltrato SMS sul numero di cellulare fornito dalla ricorrente, con il seguente messaggio "*Usa $top come codice di sicurezza per completare il bonifico europeo BU0758 di EUR 3157,58 a favore di …*"
- che l'operazione veniva autorizzata per mezzo del codice trasmesso via SMS e veniva, conseguentemente eseguito dalla Banca in favore del destinatario;

L'intermediario pertanto ha concluso per il rigetto del ricorso.

DIRITTO

Il caso sottoposto all'esame del collegio ad oggetto un'operazione di pagamento avvenuta mediante bonifico bancario tramite il sistema *home banking* da ignoti. L'intermediario afferma che tali movimenti sono stati processati tramite il sistema dinamico OTP seguito anche dall'invio da parte dell'intermediario di un SMS stante l'attivazione da parte del ricorrente di un servizio aggiuntivo di protezione fruibile via SMS in caso di operazioni anomale ì, con il quale veniva trasmesso al correntista un codice di sicurezza via SMS necessario per autorizzare l'operazione e, pertanto, esclude ogni responsabilità che, invece, il ricorrente afferma sussistere per una violazione informatica della propria posizione dovuta all'inidoneità del sistema di sicurezza.
La normativa che disciplina il caso in oggetto è il d.lgs. 27 gennaio 2010 n. 11 agli artt. 7 e ss. ed il successivo provvedimento attuativo della Banca d'Italia del 5 luglio 2011.
La fattispecie in esame è già stato oggetto di pronunce di questo Arbitro e del Collegio di Coordinamento con la pronuncia n.3498\2012 e non sembra in questo caso ci si possa discostare da questo orientamento. Ebbene -è noto- che la normativa vigente ha imposto, da un lato, agli intermediari specifici obblighi di precauzione primo fra tutti l'obbligo di garantire l'inaccessibilità dei dispositivi di pagamento a soggetti non autorizzati e dall'altro ha istituito un regime speciale di protezione a favore degli utilizzatori relativo al *favor* probatorio equilibrando normativamente, in questo modo, l'evidente squilibrio che sussiste tra prestatore e utilizzatore di un servizio di pagamento.
È chiaro che l'utilizzo del servizio di pagamento trova la propria origine nel rischio d'impresa cioè l'idea secondo la quale è razionale far gravare sull'impresa i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose" che interessano una moltitudine di consumatori spalmando, i relativi costi del rischio, sulla moltitudine degli utilizzatori: il rischio dell'impiego fraudolento di carte di credito e strumenti di pagamento ricade sui consumatori ribaltando su di essi il costo delle relative assicurazioni.
L'intermediario deve quindi adottare i più avanzati accorgimenti tecnici di prevenzione per entrare nel "porto della irresponsabilità" e far ricadere sul cliente la responsabilità il quale, avendo la disponibilità di strumenti di sicurezza, omette di avvalersene. Nel caso in esame lo strumentario offerto al cliente è consistito nella messa a disposizione dei cosiddetti *token otp* cioè un congegno in grado di generare mutevoli password monouso che, aggiungendosi alla password fissa, nota solo all'utente, concorrono a formare un sistema di autenticazione a due fattori di difficilissima forzatura e, dunque, ritenuto coerente alle indicazioni di cui al provvedimento della Banca d'Italia del 5 luglio 2011 ove si prevede che gli intermediari si attrezzino adeguatamente per identificare, valutare misurare e monitorare la natura tecnologica dei sistemi di sicurezza.
Fermo, quindi, che il metodo a due fattori con OTP risulta il più sicuro possibile, allora, l'intrusione in tali sistemi di sicurezza non può che avvenire attraverso la cooperazione, seppur involontaria, del cliente con la mancata custodia di codici dei dispositivi di autenticazione ovvero nell'ingenua trasmissione degli stessi a terzi. Pertanto, nel caso in esame, applicando anche l'orientamento di questo collegio n.1940\17, è onere del prestatore di servizi di pagamento provare che l'operazione disconosciuta è stata autenticata correttamente registrata e contabilizzata e che la sua patologia non sia dovuto a malfunzionamenti delle procedure esecutive o ad altri inconvenienti restando circoscritta la responsabilità dell'utilizzatore ai casi di comportamento fraudolento del medesimo o al suo uso gravemente colposo in adempimento degli obblighi previsti dall'art. 7 del d.lgs. 2010/11.

Tanto ricordato, osserva questo Collegio che, essendo onere dell'intermediario - onde sottrarsi alla richiesta di rimborso del cliente che neghi di aver compiuto o autorizzato le operazioni eseguite attraverso lo strumento di pagamento - quello di provare la colpa grave o il dolo del cliente titolare di tale strumento, ai fini della presente decisione, considerate le evidenze di causa, una tale prova può ritenersi raggiunta, almeno in via presuntiva. Ciò, soprattutto, con particolare riferimento alla violazione dell'obbligo del ricorrente di custodire e mantenere segrete con opportuni accorgimenti le credenziali informatiche necessarie per il regolare utilizzo del bancomat e della carta di credito.
Né il ricorrente fornisce alcun elemento anche indiziario, induttivo o indiretto utile a sollecitare almeno il sospetto di una eventuale clonazione dello strumento di pagamento.
Ebbene tale onere probatorio, nel caso di specie, risulta essere stato assolto dall'intermediario il quale afferma che le operazioni contestate sono state processate con il sistema dinamico OTP inviato sul numero di cellulare indicato riscontrabile anche nel modulo del ricorso presentato dal ricorrente.
A ciò si aggiunga che nel caso in esame dalla documentazione in atti si evince che l'accesso all'account della ricorrente è avvenuto senza che vi fossero tentativi falliti nell'inserimento di password oppure anomalie di altro genere. Intorno alle ore 9.07:57, inoltre, il servizio di internet banking rilevava una disposizione sospetta e subito inoltrava, come da didascalia, un SMS al numero associato al conto della ricorrente, contente un codice di sicurezza per completare il bonifico. Nei secondi successivi sia la password inoltrata via SMS, che la OTP generata dal servizio "O-key" venivano inserite correttamente.
Pertanto può esser revocato in dubbio che l'utilizzatore è incorso nell'inadempimento di cui all'art. 7 d.lgs 2010/11 e le relative operazioni non possono che essere addebitate al cliente.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE LEONARDO CARRIERO