Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) SANTAGATA DE CASTRO	Presidente
(NA) FEDERICO	Membro designato dalla Banca d'Italia
(NA) CAGGIANO	Membro designato dalla Banca d'Italia
(NA) PORZIO	Membro di designazione rappresentativa degli intermediari
(NA) SBORDONE	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ANDREA FEDERICO

Seduta del 19/11/2020

FATTO

Con reclamo del 06.03.2020, il ricorrente disconosceva una operazione di pagamento di euro 1.403,51 effettuata in data 02.03.2020. A seguito del mancato accoglimento del reclamo, adiva questo Arbitro e chiedeva il rimborso di euro 1.403,51.
L'intermediario depositava controdeduzioni e affermava che il ricorrente era stato vittima di *phishing* e, fermo restando, la regolare esecuzione delle operazioni e l'assenza di anomalia o irregolarità, concludeva per il rigetto del ricorso.

DIRITTO

Il ricorrente ha disconosciuto una operazione di pagamento di euro 1.403,51 e ha imputato la responsabilità della frode alle gravi carenze organizzative dell'intermediario resistente.
L'operazione disconosciuta è sottoposta alla disciplina dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno. Come statuito dal Collegio di Coordinamento (decisione n. 22745 del 10 ottobre 2019) l'intermediario resistente è gravato dell'onere probatorio previsto nei commi 1 e 2 dell'art. 10 del Dlgs 11/2010, con riguardo sia al profilo dell'autenticazione ed esecuzione delle operazioni di pagamento, sia a quello della colpa grave dell'utilizzatore. In particolare, al fine della dimostrazione della colpa grave

dell'utente, l'intermediario deve indicare gli «*elementi di fatto che caratterizzano le modalità esecutive dell'operazione*» suscettibili di fondare, in via presuntiva, la prova della colpa grave.

L'intermediario ha affermato che, a partire dal mese di giugno 2016, le carte di debito, di credito e prepagate, suscettibili di essere utilizzate per pagamenti on line, sono state abilitate al «Servizio Pagamenti sicuri internet» sì che la conferma dell'operazione di pagamento esige la digitazione di una password dinamica (OTP) tramite chiavetta 0-key ovvero, come nel caso sottoposto all'esame del Collegio, mediante APP della Banca o ricevuta tramite SMS per i clienti che hanno richiesto tale modalità, con conseguente carattere strettamente personale, in entrambi i casi, dei codici nella disponibilità del cliente.

L'operazione è stata richiesta, alle ore 10:53 del 02.03.2020, con le credenziali del ricorrente da un indirizzo IP non utilizzato in precedenti occasioni ed è stata seguita dal processo di attivazione del servizio 0-Key Smart che attraverso l'OTP software ha fornito il codice 0-Key virtuale (OTP) tramite l'APP della banca - su un telefono diverso da quello del ricorrente. Alle ore 10:53:24, l'intermediario ha inviato sms al numero di cellulare del ricorrente recante il codice per l'attivazione del servizio O-Key Smart e del seguente tenore «*Usa il codice 431684 per attivare 0-Key Smart. ATTENZIONE NON FORNIRE A NESSUNO QUESTO CODICE! Usalo solo all'interno dell'APP Mobile sul tuo telefono*». L'invio di questo messaggio ha consentito al cliente di venire a conoscenza dell'inoltro della richiesta prima dell'esecuzione. A conferma dell'abilitazione del nuovo smartphone è stato inoltrato al numero telefonico del cliente SMS di alert di seguito trascritto «*ATTENZIONE 0-key Smart è attiva su Samsung SM-J610FN Opera da questo dispositivo!*». A seguito del login dal nuovo dispositivo, è stato inoltrato al dispositivo registrato del cliente la push notification contenente il messaggio «*È stato eseguito il 02.03.2020 alle 10:54 un accesso all'App [intermediario] da un nuovo dispositivo: SM-J610FN. Non sei stato tu? Contatta la Filiale Online dalla sezione Parla con Noi*» comunicando in modo univoco l'accesso da un nuovo device. Alle ore 10:55 è stata inoltrata push notification di invito a generare l'otp virtuale, inviata al dispositivo mobile registrato (dall'ignoto richiedente) recante il messaggio «Stai autorizzando il pagamento di 1403,51 EUR presso […]», con corretta validazione dell'OTP virtuale e successivo invio di una push notification al dispositivo del cliente recante il messaggio di alert «Richiesta operazione di 1403,51 EUR con la carta 5167 * * 3107 presso ... - 02.03 ore 10:55».

Sulla base della documentazione depositata dall'intermediario resistente, a registrazione dell'App O-key Smart esigeva l'inserimento simultaneo di password statiche e dinamiche, cioè il codice titolare (password statica) il codice PIN (password statica) e il codice OTS (codice "usa e getta") inviato al cliente tramite SMS al numero di cellulare comunicato in fase di sottoscrizione del contratto e certificato dal medesimo cliente. Gli "OTS" sono stati inviati sul numero del cellulare che il ricorrente ha indicato nella denuncia e regolarmente consegnati. L'intermediario ha altresì documentato l'invio di quattro sms a distanza di poco più di tre minuti, di cui due relativi all'invio di un codice da utilizzare all'interno dell'App e due diretti alla comunicazione dell'attivazione dell'App O-Key su due dispositivi con il secondo OTS preso in carico alle ore 10:56:42. L'applicazione una volta installata sul dispositivo consente di generare, tramite una "push notification", l'OTP virtuale necessario per l'autorizzazione dell'operazione eseguita in App. Inoltre, è risultato l'invio - sui due device configurati con l'App dell'intermediario - di una "push notification" con il messaggio di accesso all'App da parte di un nuovo dispositivo, seguita da quella per l'autorizzazione dell'operazione contestata inviata sempre a entrambi i device configurati

L'intermediario ha dimostrato che le operazioni sono state effettuate in modo regolare sì

che l'operazione disconosciuta è imputabile alla violazione degli obblighi di custodia delle credenziali e del primo device registrato.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
RENATO SANTAGATA DE CASTRO