Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) TOMMASI	Membro designato dalla Banca d'Italia
(BA) BUTA	Membro designato dalla Banca d'Italia
(BA) DI RIENZO	Membro di designazione rappresentativa degli intermediari
(BA) PANZARINO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - SARA TOMMASI

Seduta del 12/03/2019

FATTO

La ricorrente, titolare di una carta di pagamento rilasciata dall'intermediario resistente, riferisce di aver subìto un addebito non autorizzato dell'importo complessivo di € 932,66 in data 12/10/2018 mediante n. 2 operazioni di ricarica di carta di pagamento e un pagamento *online*. Riferisce, altresì, di aver risposto ad una *mail* apparentemente proveniente dall'intermediario, con la quale veniva chiesto l'inserimento dei dati della carta. Dopo essersi resa conto dell'accaduto, tentava di contattare l'intermediario al fine di bloccare la carta di pagamento ma tale operazione non avveniva con successo. Pertanto la ricorrente chiede la restituzione delle somme indebitamente sottratte, dell'importo complessivo di € 932,66.
L'intermediario fa presente come la frode sia riconducibile ad una classica operazione di *phishing*, di cui la ricorrente è colpevolmente rimasta vittima. Precisa che le e-mail ricevute dalla ricorrente contenevano diversi elementi palesemente estranei a qualsiasi riferimento ufficiale dell'intermediario e, ciononostante, la ricorrente procedeva incautamente all'inserimento dei dati e codici richiesti.
In relazione alle due operazioni eseguite da applicazione mobile, l'intermediario precisa che grazie all'incauta condotta della ricorrente che inseriva credenziali di accesso, dati statici della carta (PAN CVC2 e data di scadenza) e *password* dinamiche, il "malintenzionato" è stato in grado di impostare correttamente l'applicazione mobile e procedere alle operazioni di ricarica carta con successo al primo tentativo e senza il concomitante insorgere di autorizzazioni negate. Gli errori rilevati, infatti, risalgono a data antecedente alla frode e, dunque, appaiono riconducibili all'attività della ricorrente, che

non ha completato il processo di configurazione dispositiva dell'applicazione (non è riuscita, cioè, a "creare il *wallet*") e pertanto la utilizzava solo a livello consultativo.
Precisa che dalle verifiche effettuate è stato possibile accertare la legittima esecuzione e sostanziale regolarità delle operazioni contestate. Produce all'uopo un'evidenza informatica, da cui si evince che le transazioni sono state correttamente processate e regolarmente autenticate: in particolare, la spunta verde indicherebbe che le operazioni sono state effettuate con successo al primo tentativo. Produce, altresì, la tracciatura degli SMS con OTP inviate nel giorno della frode sull'utenza della ricorrente, precisando che le *password* dinamiche ivi contenute sono servite per «rendere dispositiva la carta […] all'interno ell'*App* e a confermare il codice statico impostato dal frodatore nell'applicazione mobile scaricata sul suo *device*, per l'autorizzazione dei pagamenti disposti successivamente *in-app*». Specifica, poi, che l'SMS delle ore 13.20, conteneva l'OTP impiegato per autorizzare l'operazione on line, avvenuta attraverso il sistema di autenticazione a due fattori 3Ds.
Considerata l'adozione di un sistema autorizzativo di tipo dinamico, strutturato mediante invio con *sms* della *password* dinamica sul numero di cellulare indicato, che corrisponde a quello fornito dalla ricorrente in sede di ricorso, l'intermediario ritiene indubitabile che le operazioni contestate siano state rese possibili proprio dalla condotta tenuta dal cliente.

DIRITTO

La questione sottoposta all'attenzione del Collegio concerne l'utilizzo fraudolento di una carta di pagamento. Per la soluzione del caso di specie viene in rilievo la disciplina recata dal d.lgs. 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (c.d. PSD) e dal provvedimento di attuazione della Banca d'Italia del 5 luglio 2011. In particolare, ai fini della decisione del caso di specie, è necessario fare applicazione del disposto normativo degli artt. 7, 10 e 12 del citato decreto.
In argomento, questo Collegio richiama integralmente l'orientamento espresso dal Collegio di Coordinamento (decisioni nn. 3947/2014, 3498/2012) secondo cui la normativa istituisce "un regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori" (Coll. Coord. ABF n. 897 del 14.2.2014), i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema.
La vigente disciplina ha inteso rendere l'ambiente informatico-finanziario improntato a criteri di maggior sicurezza e affidabilità da un lato, imponendo agli intermediari, nella loro qualità di prestatori di servizi di pagamento, specifici obblighi di precauzione, primo fra tutti l'obbligo di garantire l'inaccessibilità dei dispositivi di pagamento a soggetti non autorizzati (ossia diversi dal loro legittimo titolare: cfr. art. 8, comma 1° lett. a) del cit. d. lgs. 11/2010), e, dall'altro lato, istituendo un regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori. Regime e *favor* che si sostanziano nelle seguenti concatenate proposizioni precettive (art. 10 d. lgs. cit.): a) in caso di disconoscimento di un'operazione di pagamento, è onere dell'intermediario dimostrare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata e che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; b) l'apparentemente corretta autenticazione non è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la disconosca; c) la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo

ovvero al suo doloso o gravemente colposo inadempimento agli obblighi che l'art. 7 del decreto pone a suo carico e che poi si limitano all'utilizzazione dello strumento di pagamento in conformità ai patti contenuti nell'accordo quadro che regola il servizio e alla tempestiva denuncia di furto, smarrimento, distruzione o altro uso non autorizzato dello strumento. Ove una simile responsabilità non possa affermarsi (e logicamente il correlato onere probatorio incomberà sull'intermediario prestatore del servizio), l'utilizzatore non sopporterà le conseguenze dell'uso fraudolento, o comunque non autorizzato, del mezzo di pagamento (cfr. Coll. Coord. n. 3498/12).

Ai sensi del richiamato art. 10, d. lgs. n. 11/2010, infine, il profilo della colpa dell'utilizzatore viene in rilievo soltanto allorché l'intermediario abbia fornito la prova della corretta autenticazione, registrazione e contabilizzazione dell'operazione disconosciuta dal cliente, nonché dell'assenza di malfunzionamenti. È onere dell'intermediario, inoltre, fornire la prova di aver predisposto idonei presidi a tutela della sicura operatività con gli strumenti di pagamento.

L'apparente squilibrio che le predette disposizioni determinano nel rapporto fra prestatore e utilizzatore di un servizio di pagamento trova una sua giustificazione nitidamente ricostruita in una pronuncia del Collegio di Roma, ad avviso del quale "la disciplina è evidentemente ispirata al principio del rischio d'impresa" (Coll. Roma, dec. n. 1111/2010), dal momento che il fornitore dei servizi di pagamento è in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento. L'orientamento di questo Arbitro ha trovato riscontro nella sentenza della Corte di Cassazione, 3.2.3017, n. 2950, la quale ha statuito che la disciplina speciale, in tema di strumenti di pagamento, ha esplicitato il principio generale, in tema di onere probatorio a carico del debitore professionale, nelle azioni di risoluzione contrattuale, risarcimento del danno o adempimento, "in quanto si è ritenuto che non può essere omessa la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio […]; infatti la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere" (Cass., n. 2950/17, sulla scia di Cass., 12.6.2007, n. 13777. In senso conforme, cfr., da ultimo, Cass., 12.4.2018, n. 9158).

Ora, nel caso di specie, in atti è versata copia dell'e-*mail* civetta dalla quale risulta evidente l'indirizzo del mittente e la presenza di errori ortografici e grammaticali.

Con riferimento al pagamento *online* di Euro 438,66 l'intermediario ha allegato evidenza da cui risulta l'autenticazione delle operazioni che hanno formato oggetto di reclamo; ha versato in atti documentazione attestante l'avvenuto *enrollment* della carta di pagamento al sistema autorizzativo di tipo dinamico, con richiesta *password* via SMS. E' inoltre indicato il numero di telefono associato alla carta, il quale corrisponde a quello riportato nel modulo del ricorso e nel verbale di denuncia dal ricorrente. Risulta l'invio della *password* OTP via SMS al numero di cellulare associato alla carta. L'orario di invio del SMS coincide con quello delle transazioni disconosciute.

Alla luce delle modalità riferite nel ricorso, il Collegio ritiene che, nel caso di specie, l'intrusione non autorizzata nel sistema - lungi dall'essere causata da un insufficiente grado di protezione informatica del servizio offerto dall'intermediario - appare ascrivibile a colpa grave del cliente, con conseguente utilizzo abusivo delle sue credenziali di accesso. Ed, infatti, lo stesso ricorrente sostanzialmente ammette di aver dato seguito alle istruzioni contenute nei messaggi ricevuti sulla propria casella di posta elettronica, che erroneamente credeva provenire dall'intermediario resistente.

Con riferimento alle altre due operazioni contestate, consistenti in n. 2 ricariche di altra carta di pagamento emessa dallo stesso intermediario e disposte da applicazione mobile,

per gli importi di € 248,00 ed € 246,00, dalle dichiarazioni dell'intermediario non emerge con chiarezza se, una volta installata l'applicazione su un nuovo *device*, sia richiesta una *password* dinamica OTP anche per disporre le singole operazioni di pagamento. In ogni caso, gli orari degli sms relativi all'APP (inviati tra le ore 13:14 e le 13.22) non sono compatibili con l'invio delle OTP per le singole operazioni, avvenute alle 16:20 e alle 17:36.
Con riferimento alle operazioni disposte da applicazione mobile, dunque, se la truffa non si sarebbe mai potuta compiere senza la colpevole collaborazione della ricorrente, la medesima neppure si sarebbe potuta perpetrare se l'intermediario avesse predisposto presidi di sicurezza idonei a impedire qualsiasi accesso non autorizzato al sistema di *Home banking* della cliente. La prova relativa alla predisposizione di tali presidi non è stata fornita; le conseguenze dell'utilizzo fraudolento dello strumento di pagamento devono, pertanto, essere equamente distribuite tra le parti (Collegio di Bari, decisione n. 14530/18).

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 247,00.
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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI