Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) DE CAROLIS	Presidente
(BA) CAMILLERI	Membro designato dalla Banca d'Italia
(BA) TOMMASI	Membro designato dalla Banca d'Italia
(BA) DI RIENZO	Membro di designazione rappresentativa degli intermediari
(BA) CATERINO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - SARA TOMMASI

Seduta del 28/07/2021

FATTO

La ricorrente, titolare di un conto corrente presso la banca resistente, riferisce che in data 25/4/20 veniva effettuato un accesso abusivo da parte di ignoti nel sistema di e-banking, con conseguente addebito sul conto della complessiva somma di € 4.900,00.
Afferma di essere stata contattata dal "presunto" Customer Care della banca, che le comunicava un tentativo di accesso fraudolento. Riferisce che, avendo valutato la genuinità dei referenti, anche in considerazione del fatto che conoscevano il suo numero di c/c, procedeva ad accedere al proprio internet banking tramite App, ove erano presenti due operazioni di addebito "in sospeso". Il sedicente operatore telefonico le chiedeva di bloccare tali operazioni mediante inserimento dei codici di conferma ricevuti tramite SMS, unitamente al pin.
Deduce di aver immediatamente interrotto la chiamata "insospettita dalla comunicazione anomala e dalla richiesta del numero completo della carta bancomat e del relativo codice utente" e di aver chiamato il numero verde dell'intermediario per essere certa di parlare con un operatore di filiale. Avvedutasi della natura fraudolenta dell'operazione, procedeva quindi a sporgere formale denuncia e a disconoscere le operazioni. Successivamente presentava reclamo all'intermediario.
Ritiene che la responsabilità dell'accaduto sia imputabile all'intermediario, in ragione dell'inefficacia dei sistemi di sicurezza dallo stesso adottati, che hanno permesso a ignoti di accedere all'area riservata dell'home banking della ricorrente, carpendo i suoi contatti telefonici e i riferimenti bancari e facendo "figurare come effettuate operazioni dispositive sul conto di quest'ultima" (richiama Cass. n. 9158/2018).

L'intermediario, premesso che la ricorrente è intestataria di un conto corrente abilitato al servizio di home banking, afferma che in data 25/04/2020 sono state eseguite due operazioni di ricarica di € 2.450,00 ciascuna in favore di due diverse carte prepagate.
Con riguardo alle modalità di funzionamento del servizio di internet banking richiama quanto illustrato nell'introduzione all'Analisi Disconoscimento operazioni bancarie (all. 3) e precisa di aver ricevuto la certificazione che attesta l'adozione di sistemi che offrono livelli massimi di sicurezza. Nel richiamato documento viene precisato che per l'accesso ai servizi online è richiesto l'inserimento simultaneo di password statiche e dinamiche, cioè il codice titolare, il codice PIN e il codice OTP; una volta collegati al servizio online, per autorizzare le operazioni dispositive è necessario inserire il codice dinamico OTP. Inoltre, le operazioni di tipo dispositivo riconosciute come "sospette" dal sistema antifrode, sono assoggettate ad ulteriore codice di autorizzazione denominato OTS (One Time SMS, codice "usa e getta" inviato tramite SMS al cellulare associato all'utenza del Cliente) da accompagnare al codice OTP all'atto dell'autorizzazione dell'operazione. Infine, ai clienti è data la possibilità di configurare alcune domande/risposte segrete, che potranno essere utilizzate in particolari circostanze operative per confermarne l'identificazione.
Al fine di dimostrare la corretta autenticazione delle operazioni contestate e l'assenza di anomalie, produce l'estratto delle registrazioni elettroniche effettuate in occasione dell'operatività contestata, da cui si evince che le operazioni sono state correttamente autenticate con l'inserimento dell'OTP (codice dinamico) e che non vi è stata alcuna anomalia operativa. Ritiene che le operazioni siano state impartite con il corretto inserimento di tutte le credenziali possedute dalla cliente e che, pertanto, la banca ha dovuto darne esecuzione in adempimento agli obblighi assunti contrattualmente.
Quanto alla prova della colpa grave della cliente, da fornirsi anche in via presuntiva come precisato dal Collegio di Coordinamento con la decisione n. 22745/19, ritiene che la ricostruzione dei fatti fornita dalla ricorrente sia sufficiente a dimostrare che l'esecuzione delle operazioni sia alla stessa imputabile, a causa della violazione gravemente colposa degli obblighi posti a suo carico. Ella, infatti, ha ammesso di aver ricevuto una telefonata fraudolenta, di aver inserito per ciascuna operazione il codice pin e aver trasmesso al truffatore il codice personale del proprio servizio di internet banking, ricevuto tramite sms e necessario all'esecuzione di ciascuna operazione disconosciuta.
Ritiene, inoltre, che dal tenore complessivo della telefonata ricevuta la cliente poteva avvedersi della sua natura fraudolenta, considerato anche che la stessa proveniva da un "comune numero privato".
Osserva come la truffa subita non sia particolarmente sofisticata, posto che le sue modalità non risultano assimilabili all'operatività di alcun servizio della banca. Precisa, poi, che il sistema adottato è sicuro e che la ricorrente ha totalmente ignorato i messaggi di alert inviati tramite push e sms alla sua utenza telefonica.

DIRITTO

La questione oggetto del ricorso attiene all'uso non autorizzato di uno strumento di pagamento.
Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018.
La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di

rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, co. 4, d. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, ai sensi dell'art. 10, d. lgs. n. 11/2010, "qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". Il secondo comma del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7." (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è altresì precisato che "è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

Al riguardo, il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, 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 […]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art.7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 50 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella […] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coord., decisione n. 3947 del 24.6.2014. In senso conforme: Coll. Coord. Decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014. Da ultimo, cfr. Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, co. 2, d. lgs. n. 11/2010).

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. Cass.,12.4.2018, n. 9158).
Tanto premesso in termini generali, nella specie, le operazioni oggetto di ricorso consistono in due operazioni di ricarica di € 2.450,00 ciascuna, effettuate il 25/04/2020.
L'intermediario ha allegato alle controdeduzioni un file excel di "tracciature informatiche" relative all'autenticazione, registrazione e contabilizzazione delle operazioni contestate. Trattasi di un file composto da cinque fogli, così denominati: 1) "anagrafica" (sui dati anagrafici della cliente reperiti nell'archivio del servizio internet banking); 2) "accessi" (sull'elenco degli accessi al servizio effettuati dall'utenza del cliente); 3)"tracciatura" (sulla tracciatura informatica delle operazioni disconosciute); 4) "sms" (sull'elenco dei messaggi sms inviati al numero telefonico mobile del cliente); 5) "push" (sull'elenco delle push notification inviate all'APP mobile del cliente).
Le operazioni sono state portate a termine grazie all'inserimento di un codice OTS inviato sul cellulare certificato della cliente e alla conferma di notifiche push da parte del device della ricorrente con chiave **********dbeb80.
La ricorrente riferisce di aver seguito le istruzioni fornite da un sedicente operatore telefonico dell'intermediario, entrando nell'app installata sul suo device e digitando sia i codici ricevuti tramite sms sulla propria utenza telefonica, sia il codice pin e di aver ricevuto, oltre agli sms contenenti i codici, altri due messaggi, apparentemente provenienti dall'intermediario, con i quali veniva dapprima invitata ad inserire i codici che le sarebbero arrivati al fine di "adempiere allo storno della ricarica e autorizzare la notifica che segue dopo" e successivamente avvertita del buon esito dello storno con il seguente testo: "storno ricarica e riaccredito eseguito". Non sono in atti le evidenze di tali messaggi, al fine di effettuare la verifica in merito al legittimo affidamento riposto dall'utente sulla loro genuinità e il numero di telefono indicato nella denuncia, da cui la ricorrente ha ricevuto la chiamata, non è riconducibile ai canali ufficiali dell'intermediario.
Ebbene, nel caso di specie, ritiene il Collegio che la condotta del ricorrente evidenzi, in effetti, gli estremi della colpa grave, nei termini illustrati dall'intermediario e non contestati dal ricorrente, il quale ha, per vero, sostanzialmente ammesso, in sede di denuncia, le circostanze di fatto sopra esposte. In particolare, assume rilievo la circostanza che la password OTS sia stata inviata utilizzando un diverso canale (SMS al numero di telefono del cliente), rispetto a quello previsto per l'OTP (generata dall'APP installata sul device associato al servizio O-Key Smart) e che tutti i codici di sicurezza e gli alert sono stati inviati sul dispositivo del ricorrente, poiché la frode non è avvenuta previo enrollment di altro dispositivo da parte del frodatore. Alla fattispecie in esame, pertanto, non è applicabile l'orientamento che ritiene non adeguato, ai fini della definizione delle reciproche responsabilità, il sistema di sicurezza tramite invio di OTP e OTS quando per la trasmissione di tali codici, venga utilizzato lo stesso canale, potenzialmente compromesso, ovvero uno dei due codici venga comunque ricevuto dal device del truffatore su cui sia stata installata l'app dell'intermediario (cfr., in senso conforme Collegio di Bari, decisione n. 13913/21 e n. 16422/21).

PQM

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
BRUNO DE CAROLIS