Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) GRAZIADEI	Membro designato dalla Banca d'Italia
(TO) FERRANTE	Membro designato dalla Banca d'Italia
(TO) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(TO) CATTALANO	Membro di designazione rappresentativa dei clienti

Relatore EDOARDO FERRANTE

Seduta del 17/02/2021

FATTO

Il ricorrente ha rappresentato, in sintesi, che in data 28.05.2020, intorno alle ore 14.16, riceveva un sms da un mittente riconducibile all'intermediario che lo informava di un tentativo di truffa a suo danno; che nel messaggio veniva invitato a mettersi in contatto con il reparto sicurezza; che a questo punto chiamava l'operatore che lo informava di dover procedere al blocco della carta a seguito di due tentativi di operazioni fraudolente di pagamento da parte di ignoti; che quindi procedeva secondo le istruzioni del sedicente operatore; che in data 31.05.2020 veniva nuovamente contattato dall'intermediario che lo avvertiva di un tentativo di pagamento non andato a buon fine; che in tale occasione scopriva che la carta non era stata bloccata dall'operatore telefonico e che anzi ignoti avevano effettuato un'operazione fraudolenta ai suoi danni per l'importo di Euro 800,00; che non riceveva, con riguardo a detto pagamento, alcun *sms alert* da parte dell'intermediario. Il ricorrente ha affermato pertanto di essere rimasto vittima di una frode informatica sofisticata, il c.d. *spoofing*, in quanto gli ignoti malfattori avrebbero utilizzato il recapito ufficiale della banca per l'invio degli sms e i codici di blocco, e tutte le comunicazioni ricevute dal sedicente operatore avrebbero fatto seguito allo storico delle comunicazioni genuine abitualmente inviate dalla parte resistente. Parte ricorrente ha concluso, infine, che alla luce delle circostanze, "anche adottando l'ordinaria diligenza (…) non avrebbe potuto rilevare *ictu oculi* la frode realizzata dai malviventi" e che non vi sono evidenze che l'istituto convenuto abbia agito (testualmente) "adottando le misure di prevenzione delle frodi richieste per legge e con la diligenza del buon banchiere cui è

giuridicamente obbligat[o]". Per questi fatti parte ricorrente ha sporto denuncia, con più distinte dichiarazioni, presso l'Autorità di pubblica sicurezza (agli atti).
In data 31.05.2020 il cliente ha proposto reclamo nei confronti dell'intermediario, il quale vi ha dato riscontro negativo.
Nelle controdeduzioni al ricorso, presentate tramite il Conciliatore bancario in data 18.09.2020, parte resistente, confermato che il cliente è rimasto vittima di frode, nella quale sarebbe incorso dopo aver contattato un numero telefonico contenuto in un messaggio apparentemente riconducibile allo stesso intermediario, contesta al cliente una colpa grave per aver rivelato incautamente il codice dispositivo al malfattore, nonostante il messaggio che lo conteneva rappresentasse il precipuo scopo dell'OTP; l'operazione disconosciuta si sarebbe perfezionata presso un sito che utilizza il protocollo 3DS e richiede l'inserimento di un'OTP di conferma; a seguito di utilizzi sospetti precedenti alla frode, ma non andati a buon fine, in data 28.05.2020 alle ore 14.21 e 14.22 (vale a dire "pochi minuti prima degli addebiti illeciti") avrebbe inviato sul telefono del cliente un messaggio per la verifica delle transazioni riscontrate, "chiedendo di rispondere SI nel caso riconoscesse come proprie le spese elencate nel testo del messaggio"; avrebbe subito ricevuto dal numero telefonico del cliente una risposta affermativa, sicché la carta, che era stata momentaneamente sospesa per procedure di sicurezza e per tutela dell'utilizzatore, veniva riattivata.
A dette controdeduzioni il cliente ha replicato con nota del 6.10.2020, con la quale, ad integrazione di quanto già illustrato con il ricorso, ha ribadito di non aver avuto contezza della frode e di non aver agito con colpa grave e ha osservato che l'intermediario avrebbe dovuto approntare idonee misure di sicurezza a difesa dei propri clienti.
Parte ricorrente ha domandato (testualmente) di "accertare la sussistenza del diritto (…) al rimborso integrale dell'importo di € 800,00 (…), oltre interessi dalla data di deposito e delle spese di procedura del presente ricorso"; in via subordinata, chiede la condanna dell'intermediario al pagamento delle somme illecitamente sottratte, al netto della franchigia di legge. Parte resistente ha domandato il rigetto del ricorso.
Alla riunione del 22.12.2020 questo Collegio ha sospeso il procedimento e ha disposto che parte resistente "fornisca chiarimenti circa il doppio fattore utilizzato per il compimento dell'operazione fraudolenta, fornendo idonea documentazione a supporto".
In data 21.01.2021 parte resistente, senza produrre documentazione a supporto, ha presentato una nota con la quale, anziché rispondere al quesito posto da questo Collegio, ha ribadito quanto già allegato in sede di controdeduzioni, vale a dire che parte ricorrente avrebbe fornito al malfattore i propri dati personali, il codice CVV posto sul retro della carta (di esclusiva conoscenza del titolare della carta), la data di scadenza della carta medesima e i codici dispositivi ricevuti tramite SMS dall'intermediario.

DIRITTO

La controversia verte sulla responsabilità del prestatore di servizi di pagamento in caso di loro utilizzo non autorizzato, segnatamente quando il cliente, come nel caso di specie, abbia disconosciuto un'operazione di *home banking* asseritamente eseguita, con mezzi fraudolenti, da terzi ignoti (non è però agli atti il contratto relativo allo strumento di pagamento). L'operazione contestata, indicata nel modulo di disconoscimento versato in atti da parte ricorrente, eseguita in data 28.05.2020 alle ore 15.00 per l'importo di Euro 800,00, rientra pienamente nell'ambito applicativo del D.Lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (13.01.18) del D.Lgs. 15 dicembre 2017, n. 218, di recepimento della Dir. UE 2366/2015 (c.d. "PSD2") relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al Reg. UE n. 751/2015

relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta (trova applicazione anche il provvedimento di attuazione del Titolo II del D.Lgs. 11/2010, emanato dalla Banca d'Italia il 5 luglio 2011).
Come noto l'art. 12 D.Lgs. n. 11/2010, con evidente *favor* nei confronti dell'utilizzatore, opera uno spostamento della responsabilità in capo al prestatore di servizi di pagamento per il caso di loro utilizzo fraudolento e la estende a tutte le ipotesi di violazione degli obblighi di custodia e sicurezza non caratterizzate da frode, dolo o colpa grave dell'utilizzatore. Questi infatti può sopportare le conseguenze delle operazioni fraudolente nel limite massimo della franchigia di euro 50,00, salvo il caso in cui abbia agito in frode, dolo o colpa grave, uniche ipotesi a fronte delle quali incorrerà in responsabilità illimitata (art. 12, comma 3, D.Lgs. n. 11/2010). Ai sensi dell'art. 10 D.Lgs. n. 11/2010 (e successive modifiche) il prestatore dei servizi di pagamento ha l'onere di provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata; in mancanza di detta prova esso sopporta integralmente le conseguenze delle operazioni disconosciute, senz'alcuna limitazione o franchigia. L'intenzione del legislatore, europeo e nazionale, è evidentemente quella di premere sul prestatore dei servizi perché garantisca elevati standard di trasparenza e sicurezza e patisca, almeno in linea di principio, le conseguenze sfavorevoli del loro uso fraudolento o comunque non autorizzato (cfr. tra le molte, ABF, Coll. Torino nn. 3464/18 e 6454/18).
Ora nel caso di specie l'intermediario resistente, nella sua qualità di prestatore del servizio di pagamento, ha fornito con le controdeduzioni il log dell'operazione contestata corredato da legenda, asserendo inoltre circostanze che in forza dell'art. 12 D.Lgs. 11/2010 legittimerebbero un giudizio di colpa grave a carico del cliente (la prova dell'autenticazione, registrazione e contabilizzazione non esenterebbe di per sé sola da responsabilità, come ribadito da ABF, Coll. coord. n. 22745/19: "La previsione di cui all'art. 10, comma 2, del d.lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l''autenticazione' e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente"; cfr. anche ABF, Coll. coord. nn. 5304/13 e 6168/13 e ABF, Coll. Torino n. 3373/17).
Invero, da quanto allegato e risultante in atti, l'operazione disconosciuta appare scaturita da un fenomeno di *phishing* e *vishing*, innescato da un sms e proseguito tramite contatto vocale telefonico, realizzato ai danni del cliente utilizzando il metodo del c.d. *spoofing*. In particolare, la modalità seguita dai truffatori per ottenere le informazioni dal cliente sembra riconducibile al c.d. "*SMS spoofing*", che consiste nella manipolazione dei dati relativi al mittente di un messaggio per far sì che questo appaia provenire da un soggetto differente, rimpiazzando il numero originario con un testo alfanumerico (ossia quello utilizzato dall'intermediario per i propri messaggi genuini). In tal modo, il truffatore può inviare SMS-civetta che sembrano provenienti da numeri o contatti legittimi. Nell'ambito della medesima *chat*, invero, assieme ai messaggi civetta, risulta essere pervenuto al ricorrente anche il messaggio genuino da parte dell'intermediario, contenente il codice OTP. Ora, sebbene gli elementi forniti non siano sufficienti a svolgere i necessari approfondimenti, dalla denuncia all'Autorità versata in atti dalla parte ricorrente emergerebbe una tipologia di truffa assai insidiosa, che deporrebbe in senso contrario ad una sua colpa grave.
Sennonché dalle allegazioni di parte e dalla documentazione in atti emerge un dato che, a prescindere dalla vera o supposta colpa grave del cliente, ne rende in ogni caso accoglibile la pretesa di rimborso. Non è infatti provato, allo stato, che l'intermediario abbia

allestito e concretamente attivato un sistema a doppio fattore per il compimento dell'operazione disconosciuta. Tale infatti non può considerarsi un procedimento di autenticazione basato sull'utilizzo delle sole credenziali della carta e di un codice dinamico OTP: secondo i noti standard della c.d. PSD2 e dell'EBA quest'ultimo codice rappresenta indubbiamente un utile fattore d'autenticazione, ma non così le predette credenziali, le quali in sé e per sé considerate non integrano né un elemento di conoscenza né un elemento di possesso, sicché l'impiego di queste ultime e dell'OTP dispositiva rispecchia a ben vedere un unico anziché un doppio fattore d'autenticazione.
Per orientamento condiviso dei Collegi ABF una tale deficienza, la mancanza o per lo meno la mancata dimostrazione di un procedimento pluri-fattoriale di autenticazione delle operazioni di *home banking* secondo i parametri-base della c.d. PSD2 e dell'EBA, impone in ogni caso l'accoglimento integrale del ricorso, costituendo essa un *prius* logico rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.
Spettano infine alla parte ricorrente, come da domanda, gli interessi legali dalla data del reclamo.

P.Q.M.

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 800,00, oltre interessi legali dalla presentazione del ricorso al saldo.
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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
EMANUELE CESARE LUCCHINI GUASTALLA