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) SILVESTRI	Membro di designazione rappresentativa degli intermediari
(NA) SBORDONE	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - SANTAGATA DE CASTRO RENATO

Seduta del 03/04/2019

FATTO

La ricorrente afferma che: 1) in data 17.8.2018, mentre si trovava all'estero, veniva a conoscenza di un'operazione di pagamento on line mai autorizzata, compiuta intorno alle ore 12:00 tramite il servizio di home banking da ignoti in pari data per un importo di euro 800,00; 2) provvedeva, pertanto, immediatamente a bloccare la carta intorno alle ore 12:15 tramite contatto telefonico e, rientrata in Italia, a sporgere denuncia alle autorità competenti, nella quale riferiva di aver ricevuto una mail, apparentemente proveniente dall'intermediario, in cui la si invitava a rispondere al fine di evitare il blocco del proprio account per 30 giorni e ammetteva di aver riscontrato la stessa in quanto si trovava all'estero e tutte le prenotazioni degli alloggi erano riferite alla sua carta; 3) l'accaduto è imputabile alla inadeguatezza dei sistemi di controllo dell'intermediario, in quanto non ha mai ceduto a terzi la carta ed ha tenuto un comportamento improntato alla comune diligenza (cita a supporto della sua prospettazione la sentenza della Corte di Cassazione n. 2950/2017, secondo cui la sottrazione dei codici del correntista attraverso mezzi fraudolenti rientra nell'area del rischio di impresa dell'intermediario, che deve predisporre le misure che consentano di verificare se l'operazione è attribuibile al cliente, prima di darvi corso).
Con nota di contestazione importi la ricorrente disconosceva formalmente l'operazione fraudolenta, richiedendone l'integrale rimborso; detta richiesta era rigettata dall'intermediario che, nel riscontrare il reclamo, affermava di non poter procedere al rimborso in quanto la transazione risultava legittimamente eseguita, con il corretto

inserimento delle credenziali di accesso di cui parte attorea è esclusiva titolare.
Ciò premesso, la ricorrente, assistita dal proprio legale di fiducia, ha adito l'Arbitro, al quale ha chiesto di dichiarare l'intermediario convenuto tenuto alla restituzione dell'intero importo relativo all'operazione contestata, pari ad euro 800,00, oltre le spese di assistenza difensiva, quantificate indicativamente in euro 200,00.
Costituitosi ritualmente, l'intermediario ha chiesto il rigetto del ricorso, eccependo l'assenza di ogni responsabilità nella produzione dannoso.
Parte resistente ha dedotto, in particolare, che la questione sottoposta all'ABF è da inquadrare nella particolare forma di frode nota come phishing classico, come attestato dalla dinamica indicata nel ricorso, ed ha osservato che il contenuto insolito della comunicazione avrebbe dovuto allertare la ricorrente poiché non è sua consuetudine inviare richieste di dati alla clientela per ovviare all'inconveniente di un blocco praticato su un conto corrente o una carta in seguito a rilevate anomalie. Peraltro, la tracciatura informatica dell'operazione contestata consente di affermare che la stessa è stata correttamente autenticata al primo tentativo e processata con il sistema di autenticazione a due fattori: inserimento nel sito delle credenziali statiche della carta (PAN, CVC2 e data di scadenza) e adesione al protocollo 3Dsecure che prevede l'utilizzo del sistema dinamico OTP, con invio di sms sul numero di cellulare indicato dalla ricorrente a parte resistente, uguale a quello risultante dalla denuncia alle autorità competenti. L'intermediario ha altresì richiamato, a supporto della propria prospettazione, la decisione del Collegio di Coordinamento. n. 3498/12, escludendo ogni responsabilità nella produzione dell'evento dannoso anche perché: a) è stato sempre proattivo nell'informare la clientela sui temi della sicurezza degli strumenti di pagamento attraverso apposite informative diffuse presso tutti i canali di contatto con il pubblico, nei quali si invita sempre a non fornire mai i dati personali e quelli relativi ai dispositivi di pagamento tramite telefono, email o sms, perché nessuna banca o altro ente li richiede mai ai propri clienti; b) ha messo a disposizione del cliente un sistema di autenticazione a due fattori, che tuttora rappresenta la tecnologia reputata più avanzata ed affidabile nell'ambito dei pagamenti on line.
La ricorrente ha depositato repliche alle controdeduzioni dell'intermediario, in cui contesta la ricostruzione operata da quest'ultimo, rilevando che lo stesso non ha adempiuto al proprio onere probatorio e si è invece limitato a mere considerazioni di carattere probabilistico ed a mere asserzioni rimaste, peraltro, prive di adeguato riscontro: tali considerazioni valgono sia in relazione alla presunta negligenza della correntista, sia con riferimento all'asserito proprio rispetto degli obblighi di diligenza professionale richiesti dall'art. 1176, comma 2 c.c. A supporto della propria prospettazione cita l'ordinanza della corte di Cass. 12 aprile 2018, n. 9158, secondo cui l'eventuale uso dei codici di accesso al sistema da parte dei terzi rientra nel rischio professionale del prestatore dei servizi di pagamento, che devono predisporre idonee misure per evitare tale eventualità; pertanto, qualora si verifichi un accesso non autorizzato o l'impiego dei dati raccolti per finalità non conformi alla legge, il gestore risponde ex art. 2050 c.c: si tratta di una forma di responsabilità oggettiva "aggravata", in cui il prestatore del servizio, per andare esente da responsabilità, non deve solo dimostrare di aver adottato tutte le misure idonee ad evitare il danno (cosiddetta "prova liberatoria"), ma è tenuto a fornire la prova positiva di una causa esterna. L'istante ha altresì puntualizzato che, nel caso di erogazione del servizio di home banking, la banca è tenuta a garantire uno standard di sicurezza adeguato nell'effettuazione dei pagamenti al fine di precludere l'accesso a soggetti non abilitati al sistema: la diligenza richiesta, in tale circostanza, ha natura tecnica (art. 1176, c. 2, c.c.) e va valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere.

DIRITTO

Oggetto del ricorso è la richiesta di restituzione del complessivo importo di un'operazione di acquisto effettuata on line, tramite il servizio di home banking, da ignoti per un importo di euro 800,00.
La questione del disconoscimento di operazioni dispositive, effettuate online, delle quali si afferma il carattere fraudolento, più volte posta all'attenzione dell'Arbitro, è stata risolta in base a due fondamentali elementi di giudizio: per un verso, la valutazione dell'adeguatezza sia del sistema di protezione delle transazioni online adottato dall'intermediario sia della sua organizzazione, funzionale alla segnalazione ed al blocco di eventuali operazioni anomale, quali espressioni della diligenza professionale dallo stesso esigibile ai sensi dell'art. 1176, comma 2, c.c.; per altro versante, l'osservanza, da parte dell'utilizzatore dei servizi di pagamento, delle disposizioni previste dagli artt. 7 e 9, d.lgs. 11/2010.
È noto che tale disciplina mira a salvaguardare l'utente dei servizi di pagamento, come attestano: 1) la c.d. inversione dell'onere della prova in tema di responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento (art. 12, d.lgs. 11/2010, nel testo modificato dal d.lgs. 218/2017); 2) il dovere del prestatore del servizio di pagamento di "assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento, fatti salvi gli obblighi posti in capo a quest'ultimo ai sensi dell'articolo 7" (art. 8, d.lgs. 11/2010, nel testo modificato dal d.lgs. 218/2017).
In particolare, l'utilizzatore è tenuto alla rigorosa osservanza di una serie di obblighi, che vanno dalla custodia delle credenziali di autenticazione, all'adozione, secondo diligenza, delle normali cautele che è ragionevole attendersi nell'uso dello strumento di pagamento (art. 7, d.lgs. 11/2010, nel testo modificato dal d.lgs. 218/2017).
Ebbene, l'adeguato assolvimento degli obblighi previsti dalla vigente disciplina in tema di sicurezza degli strumenti di pagamento vale ad esonerare dalla responsabilità per i danni subiti dall'utilizzatore del servizio di pagamento, così come emerge dall'art. 12, commi 2° e 2-bis: "Salvo il caso in cui abbia agito in modo fraudolento, l'((utente)) non è responsabile delle perdite derivanti dall'utilizzo dello strumento di pagamento smarrito, sottratto o utilizzato indebitamente quando il prestatore di servizi di pagamento non ha adempiuto all'obbligo di cui all'articolo 8, comma 1, lettera c). Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente. Salvo il caso in cui abbia agito in modo fraudolento, l'utilizzatore non è responsabile delle perdite derivanti dall'utilizzo dello strumento di pagamento smarrito, sottratto o utilizzato indebitamente quando il prestatore di servizi di pagamento non ha adempiuto all'obbligo di cui all'articolo 8, comma 1".
Ebbene, nel caso di specie, al Collegio paiono determinanti per la soluzione della controversia le particolari modalità di esecuzione dell'operazione contestata, riferite dalla stessa ricorrente nella denuncia del 29.8.2018, ove quest'ultima ha affermato di aver ricevuto una mail, apparentemente proveniente dall'intermediario, che la invitava a rispondere al fine di evitare il blocco della carta per 30 giorni e di averla riscontrata dato che si trovava all'estero e che tutte le prenotazioni degli alloggi erano riferite alla citata carta. Questa circostanza vale di per sé a rendere evidentemente non sovrapponibile la fattispecie in esame a quella esaminata dalla Cass., 12 aprile 2018, n. 9158 (citata dalla ricorrente), in cui era invece assente "qualunque obiettivo riscontro di rilievo pure

indiziario" della responsabilità dei clienti.
Dal canto suo, l'intermediario ha prodotto la tracciatura informatica della modalità di esecuzione della transazione che afferma essere stata eseguita senza alcuna anomalia, risultando la disposizione di pagamento regolare, come confermato dalla spunta verde accanto alla stessa. Il che non consente allora di equiparare il caso in questione alla fattispecie esaminata dalla Cass., 3 febbraio 2017, n. 2950, in cui l'intermediario non aveva fornito alcuna dimostrazione in ordine all'idoneità del sistema di sicurezza adottato in quanto l'odierna resistente, nella fattispecie in esame, ha dimostrato invece di aver utilizzato un sistema che, da questo Collegio, è stato più volte riconosciuto adeguato ed idoneo ad assicurare alla clientela una "protezione rafforzata" (cfr., fra le tante, ABF Napoli, nn. 4397/2014 e 8292/2014) e non v'è ragione di discostarsi, in questa occasione, da tale consolidato orientamento.
Del resto, dalla stessa denuncia della ricorrente, emerge chiaramente che la stessa è rimasta vittima di una colpevole credulità: colpevole in quanto ella è stata portata a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità, quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di Internet (cfr. Collegio di Coordinamento, n. 3498/2012).
Pertanto, il Collegio deve inquadrare la fattispecie in esame nel c.d. "phishing": di tal ché, l'intrusione non autorizzata nel sistema – lungi dall'essere causata da un insufficiente grado di protezione informatica del servizio offerto dall'intermediario – appare piuttosto ascrivibile a colpa grave della cliente, con conseguente utilizzo abusivo delle sue credenziali di accesso (in termini, ad es., ABF Roma, n. 13448/2017; ABF Napoli, nn. 5488/2019 e 11243/2017).
In considerazione di quanto precede, il ricorso non può essere accolto.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE LEONARDO CARRIERO