Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

IL COLLEGIO DI NAPOLI

composto dai signori:

- prof. avv. Enrico Quadri ..... Presidente
- avv. Giuseppe Leonardo Carriero ..... membro designato dalla Banca d'Italia
- prof. avv. Giuseppe Conte ..... membro designato dalla Banca d'Italia
- prof.ssa Marilena Rispoli Farina ..... membro designato dal Conciliatore Bancario Finanziario (estensore)
- prof. avv. Andrea Barenghi ..... membro designato dal Consiglio Nazionale Consumatori e Utenti

seduta del 26.2.2013

- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario e la relativa documentazione;
- la relazione istruttoria della Segreteria tecnica

FATTO

Il 25/1/12 alle ore 18:50 circa, la ricorrente, titolare di un conto corrente postale attivato presso la resistente, veniva contattata dal Servizio Antifrode dell'intermediario per ottenere conferma dell'avvenuta autorizzazione, in quella giornata, di due operazioni di ricarica a favore di carte prepagate di soggetti terzi, altresì rilasciate dalla resistente. La ricorrente, dopo esserci sincerata che nemmeno l'altro cointestatario avesse autorizzato le operazioni de quo, ne effettuava il disconoscimento.
Il giorno successivo, si recava presso la filiale dell'intermediario competente, ove apprendeva che sul proprio conto erano state addebitate tanto le due operazione indicate quanto analoga operazione (occorsa il 23/1/12) di ricarica di altra prepagata, tutte di importo pari ad € 500,00. Provvedeva pertanto a sporgere denuncia alla P.S. e, in tale sede, dichiarava che tre giorni prima, nel corso di una navigazione internet, "ancora prima di fare accesso" al sito ufficiale dell'intermediario, al cointestatario era apparsa una pagina web raffigurante i loghi dell'intermediario e che, su specifica richiesta, aveva inserito la carta associata al conto nell'apposito lettore rilasciato dalla resistente, il PIN ed il codice generato dal lettore. "Dopodiché faceva accesso al conto corrente online".
Il 2/7/2012 il ricorrente inoltrava alla resistente richiesta di restituzione delle "somme attualmente congelate (€ 1.500,00)", ma tale reclamo restava privo di riscontro. Veniva pertanto adito l'ABF.

La resistente ha evidenziato che, in relazione al servizio di Internet Banking BPOL, a sua volta associato al conto corrente del ricorrente il 24/1/2008, al correntista veniva consegnato, in data 30/12/2009, il c.d."*lettore PCR*", ossia il dispositivo necessario ad autorizzare, mediante carta, le operazioni *on line.* Tale dispositivo permette, insieme con la carta abbinata al conto, dotata di *microchip*, la generazione e lo scambio di codici univoci "usa e getta" tra il sito web e il correntista al fine di verificarne l'identità al momento della disposizione di una transazione *on line*;
La resistente specificava che, dalle evidenze informatiche, le operazioni contestate risultavano effettuate mediante il corretto inserimento di tutti i codici identificativi indispensabili per l'esecuzione delle transazioni (*username* e *password* per il *login* al sito), e soprattutto con l'utilizzo del suddetto lettore, che, per sua natura, non si presterebbe ad abusi per via elettronica o informatica, prevedendo operazioni prettamente materiali. Precisava, inoltre, che i suoi sistemi informatici risultavano inviolati e assolutamente sicuri.
A fronte della totale assenza di riferimenti da parte del ricorrente in ordine alla sua postazione informatica (che a parere dell'intermediario poteva essere stata oggetto di *malware*) e considerato il corretto inserimento dei codici di accesso, noti solo al titolare, la resistente supponeva che qualcuno avesse posto in essere la sequenza di atti prescritti per il perfezionamento delle transazioni con uso della specifica carta, e che quindi lo stesso ricorrente avesse incautamente e inconsapevolmente fornito a terzi il codice dispositivo così generato (ad es. accedendo ad un sito *internet* solo in apparenza appartenente all'intermediario ed ivi digitando i dati riservati). La resistente riteneva, pertanto, che le due operazioni *on line* erano riconducibili al comportamento negligente del ricorrente che, dunque, non era stato in grado di assicurare un'adeguata protezione dei propri dispositivi di connessione e dei propri dati identificativi, imputando allo stesso una responsabilità contrattuale.
L'intermediario, inoltre, escludeva la sussistenza di una propria responsabilità contrattuale ex art.1218 c.c. (tra l'altro non oggetto di contestazione da parte del ricorrente né tantomeno provata ex art 2697 c.c.) atteso che le operazioni in oggetto erano state disposte con il corretto inserimento dei dati identificativi del titolare cosicché l'intermediario, conformandosi alle condizioni contrattuali, vi aveva dato adeguata esecuzione con la diligenza qualificata richiesta.
La resistente richiamava, inoltre, per mero scrupolo difensivo, le numerose campagne di informazione e sensibilizzazione alla clientela volte alla protezione dei dati di accesso e alla prevenzione dal fenomeno di *phishing*. Rinviava, altresì, ad alcune sentenze in materia quali, tra le altre, Giudice di Pace di Potenza nella causa R.G. 18/2011 , Tribunale di Venezia n. 626/2012, e ancora Tribunale di Roma n.13266/2012;
In sede di repliche, la ricorrente asserisce di aver "adempiuto a tutti gli obblighi e/o accorgimenti previsti nelle condizioni contrattuali e [che] nessuna responsabilità può, quindi, esserle ascritta in ordine a quanto accaduto".
Soggiunge che "nonostante l'immediatezza con cui ci si è attivati, la società convenuta è rimasta assolutamente inerte e, quando è stata ricontattata per avere notizie dello stato della pratica, comunicava di aver smarrito i relativi documenti".
In conclusione, mentre il ricorrente ha chiesto il rimborso di € 1.500,00, pari alla somma degli importi delle operazioni disconosciute, la resistente ha chiesto il rigetto del ricorso, invocando le disposizioni contrattuali che prevedono l'obbligo di eseguire le disposizioni impartite mediante l'utilizzo dei corretti codici dispositivi, nonché l'art.1227, co. 2 c.c., sull'evitabilità del danno attraverso la tenuta di una condotta diligente.

DIRITTO

Il Collegio è chiamato a decidere su un ennesimo caso di prelievo fraudolento posto in essere a danno della ricorrente, titolare di un conto corrente on line presso l'intermediario resistente. La questione oggetto del presente ricorso (ripartizione delle responsabilità in presenza di un sistema di autenticazione a due fattori), è stata più volte esaminata nei confronti della medesima resistente, in casi sostanzialmente analoghi a quello in esame.
Come in precedenti decisioni (si veda, da ultimo, Collegio ABF di Napoli, decisione n. 503/2013) il Collegio rileva che la responsabilità del prestatore dei servizi di pagamento per le operazioni non autorizzate, è da valutare alla stregua dei principi generali (art. 1176, comma 2, c.c.), ma anche alla luce della disciplina speciale introdotta dalla direttiva sui Servizi di pagamento e dalla sua attuazione nell'ordinamento interno attraverso l'art.11, comma del D.Lgs. n.11 del 2010, che impone la prestatore dei servizi di "rimborsare l'importo dell'operazione", salvo l'ipotesi di dolo o colpa grave dell'utilizzatore del servizio.
In generale, da parte della giurisprudenza dell'ABF, si è rilevato che, quando l'intermediario abbia adottato dispositivi personalizzati che non consentono a terzi l'accesso a strumenti di pagamento dell'utilizzatore, come prescrive la legge, viene meno ogni possibile presunzione di colpevolezza dell'intermediario e diviene più rigorosa la valutazione dell'obbligo di diligenza dell'utilizzatore nel custodire i dispositivi di identificazione che l'intermediario gli fornisce.
In proposito, il Collegio di Napoli ha ritenuto che la recente disciplina abbia creato un sistema bilanciato di obblighi tra le parti del rapporto, ed un corrispondente regolamento delle rispettive responsabilità, imponendo all'intermediario l'obbligo di garantire la sicurezza degli interessi dell'utilizzatore (art. 8 lett. a) e all'utilizzatore l'obbligo di custodire diligentemente le proprie credenziali di accesso ai servizi di home banking (art. 7 n. 2). L'adempimento del proprio obbligo da parte di uno dei soggetti del rapporto depone, allora, nel senso dell'esclusione della sua responsabilità per le conseguenze dell'eventuale operazione fraudolenta perpetrata. Questo Collegio ha al riguardo concluso che l'adozione da parte dell'intermediario di valide ed efficaci misure di tutela degli interessi dell'utilizzatore, se non può ritenersi valere ad escludere senz'altro la sua responsabilità e, di riflesso, a dimostrare che l'intromissione fraudolenta nel sistema di protezione da lui predisposta sia imputabile alla grave (in rapporto alla massima sicurezza offerta dall'intermediario) negligenza o imprudenza dell'utilizzatore (per non avere custodito adeguatamente le proprie credenziali: art. 12, n. 4), vale sicuramente ad elevare in modo significativo il livello delle allegazioni richieste al cliente, al fine di rendere adeguatamente verosimigliante il carattere fraudolento dell'operazione.
Sul punto, va segnalato l'orientamento espresso dal Collegio di coordinamento, il quale ha svolto talune considerazioni in ordine alle divergenti valutazioni operate dai Collegi territoriali in presenza di sistemi di autenticazione a due fattori. Più precisamente, il Collegio di coordinamento (dec. n. 3498/12), aderendo sostanzialmente alla prospettiva seguita da questo Collegio, ha ritenuto che l'utilizzo di un sistema rafforzato non consente comunque alcuna presunzione assoluta circa la sussistenza di una colpa grave in capo al ricorrente.
Nel caso in esame, come si è già rilevato, l'intermediario, per rendere massimo il sistema di protezione dell'utente e particolarmente difficile all'eventuale terzo non autorizzato di penetrare nel sistema telematico ha adottato un sistema di sicurezza rafforzato. Trattasi di un "lettore" elettronico, di cui il ricorrente era in possesso, in grado di leggere il certificato di sicurezza personale che risiede nel microchip di una carta. La carta, inserita nel Lettore ed in combinazione con il PIN, consente di generare un codice "usa e getta" (c.d."one time password" o OTP) necessario per l'esecuzione delle operazioni dispositive.

La cliente, tuttavia, nel rilevare il carattere fraudolento delle operazione contestate nell'accesso al conto, ha dichiarato di non aver mai ceduto la carta ad altri, né tantomeno i codici segreti. Essa, soprattutto, ha anche dichiarato di essere stata contattata proprio dal servizio antifrodi dell'intermediario, per sapere se aveva autorizzato le operazioni di ricarica di carte prepagate a favore di terzi, quelle operazioni che il giorno successivo aveva constata effettivamente poste in essere sul suo conto. A rafforzare gli elementi che possono far propendere per una responsabilità della banca, la ricorrente, nelle repliche, ha anche evidenziato che mentre essa si era attivata con immediatezza nell'operare le contestazioni, la banca, ricontattata per conoscere l'esito del reclamo, aveva dichiarato di aver smarrito la documentazione a fondamento di tale asserzione. Pertanto, deve ritenersi che infondatamente la resistente ha concluso che l'operazione on line deve ragionevolmente presumersi riconducibile al comportamento gravemente negligente della ricorrente, che non sarebbe stata in grado di assicurare un'adeguata protezione dei propri dispositivi di connessione e dei propri dati identificativi, così violando le disposizioni di legge e di contratto in materia.
In effetti, l'intermediario, come si è rilevato, ha adottato un sistema di sicurezza "rafforzato", per evitare le frodi informatiche, ma ciò, evidentemente, alla luce della dinamica caratterizzante la vicenda in esame, non è bastato ad evitare intrusioni estranee. La ricorrente, in particolare, ha allegato circostanze che valgono ragionevolmente ad escludere, da parte sua, il dolo o la colpa grave, mentre ha invece evidenziato un comportamento scarsamente coerente e, in ultima analisi, poco diligente dell'intermediario
Pertanto, in una prospettiva tendente a valorizzare con riferimento al caso concreto le circostanze ed i comportamenti delle parti, questo Collegio ritiene che la responsabilità possa essere, nel caso di specie, riconosciuta a carico dell'intermediario.

P.Q.M.

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione della somma di € 1.500,00.
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
ENRICO QUADRI