Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) BERTI ARNOALDI VELI	Membro designato dalla Banca d'Italia
(BO) DI STASO	Membro designato dalla Banca d'Italia
(BO) LUCARELLI	Membro di designazione rappresentativa degli intermediari
(BO) PETRAZZINI	Membro di designazione rappresentativa dei clienti

Relatore CATERINA LUCARELLI

Seduta del 25/06/2019

FATTO

Titolare della carta di credito n. *155 rilasciata dall'intermediario resistente, parte ricorrente, anche a mezzo della documentazione acclusa al ricorso, riferisce che in data 04.12.2018 in tarda serata riceveva sulla propria utenza telefonica un sms di notifica dell'intervenuta variazione del numero di telefono associato allo strumento di pagamento, con contestuale invito a contattare il servizio clienti ove la suddetta variazioni non fosse stata dalla stessa autorizzata. Prontamente la ricorrente provvedeva a contattare il servizio il clienti, disconoscendo la paternità della comunicata modifica e chiedendo il blocco dello strumento di pagamento; tuttavia, nelle more, la carta di credito veniva utilizzata per effettuare una operazione di pagamento non autorizzata di importo pari a 450,00 € in favore di un beneficiario sconosciuto.

Sporta denuncia e inoltrato reclamo a mezzo di apposito modulo di contestazione, rimasto infruttuoso, inoltra ricorso all'Arbitro Bancario Finanziario chiedendo la restituzione dell'importo di euro 450,00 oltre al rimborso delle spese del procedimento.

Convenuto ritualmente, l'intermediario contro-deduce, in particolare, quanto segue:

- in data 04.12.2018, alle ore 22.03, la ricorrente riceveva un sms volto ad informala

dell'avvenuta modifica del numero di telefono associato alla carta di credito e, conseguentemente, chiamava il servizio clienti per chiedere il blocco dello strumento di pagamento, blocco che avveniva alle ore 22.10, ma alle ore 22.07, veniva eseguita un'operazione di pagamento on line per un importo pari a 450,00 €;

- la ricorrente erroneamente sporge denuncia riferendo che la transazione fraudolenta è stata eseguita a causa della clonazione della propria carta di credito, la quale, invece, è stata semplicemente utilizzata on line dopo aver effettuato l'accesso al Portale Titolari e modificato l'utenza telefonica associata alla carta;

- a fronte della suddetta ricostruzione dei fatti, emergerebbe che l'autore della frode ha avuto libero accesso anche alla casella di posta elettronica del ricorrente.

Per questo l'intermediario, in ragione del difetto di custodia delle credenziali personali, chiede all'ABF di non accogliere il ricorso.

Parte ricorrente replica alle controdeduzioni, in particolare lamentando la mancata predisposizione da parte dell'intermediario del sistema di "autenticazione forte" in fase di accesso al Portale Titolari, prevedendo la generazione e l'invio di OTP solo quando viene effettuato un cambiamento dei dati forniti oppure quando si pone in essere un'operazione di pagamento on line ma non anche quando si accede al Portale Titolari; aggiunge, poi, che l'operazione contestata configura palesemente un'ipotesi di fattispecie illecita perpetrata ai danni della stessa, come si evince dal fatto che l'accesso al portale risulta essere stato eseguito connettendosi da un indirizzo IP localizzato a XXX, mentre la ricorrente risiede e lavora in diversa regione italiana dove si trovava la sera del 04.12.2018. Quindi chiede la rifusione delle spese legali oltre accessori di legge.

DIRITTO

ABF ha più volte affermato che nelle controversie relative ad un utilizzo fraudolento di strumenti di pagamento, occorre valutare, da un lato, la condotta dei clienti con riguardo agli obblighi di diligenza nella custodia dello strumento di pagamento e dei dispositivi collegati, dall'altro, la condotta dell'intermediario, il quale è chiamato ad adempiere al mandato secondo la diligenza professionale e qualificata dell' art. 1176, comma 2, c.c. ; circostanze, queste, da valutare caso per caso (Collegio di Roma, decisione n. 10212/16).

Nel caso oggetto di questo ricorso, parte ricorrente disconosce un'unica operazione di pagamento eseguite on line nei confronti di un beneficiario sconosciuto, ovvero l'operazione di pagamento di 450,00 €, eseguita in data 04.12.2018, alle ore 22.07. A sostegno del ricorso, parte ricorrente produce: 1) lettera di contestazione del 6.12.2018; 2) denuncia; 3) denuncia del 06.12.2018; 4) estratto conto del mese di dicembre 2018 allegato alla denuncia; 5) reclamo; 6) schermata dell'accesso al portale; 7) screenshot del cellulare dimostrativo della chiamata in uscita al servizio clienti del 6.12.2018 alle ore 22:04; 8) informazioni sull'indirizzo IP da cui è avvenuta l'operazione.

L'intermediario, dal suo conta, oltre produrre evidenza documentale del pagamento disconosciuto, concentra la sua linea difensiva sui presidi di sicurezza adottati per la modifica tramite Portale Titolari dell'utenza telefonica associata alla carta di credito, che avviene inserendo l'OTP inviato sulla e-mail della ricorrente dichiarato all'atto della registrazione al portale stesso. L'intermediario allega evidenza documentale della generazione OTP per la variazione utenza telefonica inviato a mezzo e-mail associato alla ricorrente.

Alla luce delle caratteristiche tecniche di sicurezza adottate dall'intermediario e provate come attive nel caso in oggetto, il Collegio ritiene che l'operazione fraudolenta non possa essere riportata alle sue responsabilità, dal momento che la disposizione della modifica del numero di telefono attraverso una OTP inviata alla cliente via e-mail ha fornito all'intermediario un elemento positivo e concreto di autenticità del cambio del numero che ha giustificato l'esecuzione della successiva operazione di acquisto. Secondo il Collegio, il fatto che nel caso specifico l'intermediario ha inviato alla cliente una email contenente un codice di sicurezza dinamico per la finalizzazione del cambiamento del numero di telefono, a cui è spedito poi l' OTP dispositivo, è segno di robustezza del presidio di sicurezza predisposto.

D'altro lato, la condotta della ricorrente appare caratterizzata da grave negligenza in relazione sia alla custodia delle credenziali di accesso al portale, sia in relazione all'accesso alla propria posta elettronica ed al controllo della stessa. Peraltro, il fatto che la ricorrente abbia contatto l'intermediario per il blocco della carta non è un elemento che fa ritenere che l'operazione fraudolenta si potesse evitare, visto che la telefonata è iniziata alla 22:04, appena tre minuti prima dell'operazione stessa, avvenuta alle 22:07.

Tutto considerato, questo Collegio non può ritenere il ricorso meritevole di accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARCELLO MARINARI