Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BLANDINI	Membro designato dalla Banca d'Italia
(NA) PRINCIPE	Membro designato dalla Banca d'Italia
(NA) SILVESTRI	Membro di designazione rappresentativa degli intermediari
(NA) GIGLIO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ANTONIO BLANDINI

Seduta del 26/02/2019

FATTO

La ricorrente in data 05.04.2018 alle 10:38 contattava l'intermediario tramite uno dei suoi canali di comunicazione on line (una chatbox via Facebook Messenger) per un problema di attivazione di una carta di credito aggiuntiva. In risposta veniva informata che sarebbe stata ricontattata da un'agente per assisterla nella risoluzione del problema. Alle ore 10:55 sempre via Facebook Messenger la ricorrente riceveva una comunicazione che la invitava, per ricevere assistenza, ad inviare una PEC all'indirizzo fornito. Quindi la ricorrente riceveva un SMS alle ore 12:49 con il quale veniva informata che sarebbe stata contattata da un operatore alle ore 14:00. Di seguito alla telefonata effettivamente avvenuta intorno alle 14:00 una persona, qualificatasi come operatore dell'intermediario, invitava la ricorrente a inviare la richiesta della carta firmata e la copia fronte/retro della carta di credito attiva in suo possesso. Tale invito veniva ribadito tramite SMS delle ore 14:37. La ricorrente adempiva alla richiesta il 09.04.2018 alle ore 16:03. Alle ore 18:12 riceveva un SMS con il quale veniva chiesto l'invio della password personale per l'attivazione della carta ad un numero telefonico, a cui però non si dava risposta. Alle ore 18:46 e alle ore 18:48 la ricorrente riceve 2 SMS ALERT per 2 pagamenti rispettivamente di € 1.379,98 e di € 100,00 non effettuati dalla ricorrente, la quale provvedeva tempestivamente a segnalare telefonicamente a un operatore della banca i pagamenti non autorizzati. La carta veniva quindi bloccata in seguito alla chiamata. In data 10.04.2018 la ricorrente effettuava denuncia contro ignoti presso la competente autorità di polizia.

La ricorrente chiede la restituzione di € 1.379,98 e di € 100,00 corrispondenti all'importo di 2 operazioni disconosciute a seguito di asserita clonazione dello strumento di pagamento.
L'intermediario si oppone alle pretese del cliente, sostenendo:

- che le operazioni contestate elencate nel modello presentato dalla ricorrente sono state autenticate, correttamente registrate e contabilizzate, nonché eseguite nei limiti del plafond della carta di credito. Le operazioni disconosciute sono inoltre state eseguite su siti internet i cui esercenti sono stati censite "sicuri" (FULL 3D) e certificati ad effettuare solo operazioni che necessitano l'autenticazione del partecipante;
- che le operazioni sono state eseguite tramite sistema di protezione antifrode 3D Secure – Verified by Visa, il quale prevede l'inserimento dei dati della carta e della password personale segreta stabilita dal cliente;
- che il servizio di sms alert risultava essere correttamente attivo alla data di disposizione delle operazioni contestate;
- che, sulla base di quanto dichiarato dalla ricorrente sia in fase di contestazione sia in fase di ricorso, l'utilizzo non autorizzato dello strumento di pagamento è avvenuto a seguito della diffusione a terzi dei codici della carta di credito. Nel caso in esame appare evidente che la ricorrente sia incorsa in una fattispecie di "phishing" facilmente riconoscibile con un minimo di diligenza. La ricorrente è stata, infatti, invitata ad inviare copia fronte/retro della propria carta di credito attiva ad un indirizzo PEC chiaramente non riconducibile alla Banca. Inoltre la ricorrente avrebbe dovuto insospettirsi della richiesta di invio fronte/retro di una carta attiva al fine di attivare una nuova carta di credito;
- che pur non avendo dato seguito alla richiesta del 09.04.2018 (18:12) all'invio, ad un numero telefonico specificato, della password personale per l'attivazione della carta di credito, in quanto insospettita, non ha immediatamente bloccato la carta consentendo la disposizione delle operazioni contestate effettuate dopo più di 30 minuti da tale richiesta,
- che la banca, al fine di prevenire il fenomeno "phishing", ha tra l'altro ampiamente informato la propria clientela, fornendo utili indicazioni su come riconoscere un tentativo di phishing tramite appositi avvisi pubblicati sul proprio sito internet;
- che è ravvisabile una violazione gravemente colposo degli obblighi di conservazione della carta di credito statuiti nelle Norme Contrattuali.

Con le proprie repliche la ricorrente tiene a specificare che la PEC dalla stessa inviata in data 05.04.2018 alle ore 11:20 all'indirizzo comunicatole non conteneva alcun dato sensibile legato alla propria carta di credito. L'SMS ricevuto alle ore 12:49 che la informava che sarebbe stata contattata da un operatore della Banca alle 14:00 proveniva dallo stesso numero dal quale riceveva normalmente le comunicazioni relative al proprio conto corrente e carta di credito, come pure il successivo delle 14:37. La ricorrente asserisce di non avere dato seguito a quanto richiesto dal successivo SMS delle 18:12, in quanto impossibilitata e non insospettita, reputandolo veritiero. Invece subito dopo aver ricevuto gli SMS di autorizzazione ai pagamenti la ricorrente ha prontamente chiamato un operatore della Banca per bloccare la carta. Inoltre, pur avendo inviato copia fronte/reto della carta di credito non ha mai provveduto a confermare nessuno dei 3 acquisti contestati tramite password personale e che quindi il sistema "3D Secure verified by Visa" è stato aggirato in qualche modo.
In sede di controrepliche l'intermediario rinnova quanto indicato in sede di controdeduzioni, ribadisce che la responsabilità dei fatti lamentati è totalmente ascrivibile al comportamento della ricorrente che ha diffuso a terzi i codici della carta e conferma quanto richiesto all'Arbitro.

DIRITTO

La ricorrente produce in atti tutti gli elementi utili alla puntuale ricostruzione dei fatti. Innanzitutto, la stampa di una videata recante i messaggi scambiati con l'operatore virtuale, attraverso la funzione di messaggistica attiva sul profilo facebook dell'intermediario

Nell'ambito della conversazione prodotta in atti, la ricorrente riceve un primo messaggio che la rimanda ad un successivo contatto con un agente dell'intermediario e, da ultimo, un ulteriore che la invita a contattare telefonicamente il servizio clienti, data l'impossibilità di "accedere" alla posizione personale tramite quel canale di comunicazione.

Con altra videata, parte attrice fornisce evidenza di altra conversazione intrattenuta a mezzo servizio di messaggistica di facebook, con un terzo utente del social network – tal M.F. - che si presentava come agente dell'intermediario.

Tanto premesso, non è chiaro come tale sedicente agente sia entrato in comunicazione con l'odierna ricorrente: quest'ultima riferisce che, a prendere contatto, sarebbe stato lui, avendo evidentemente avuto illegittimamente accesso alla corrispondenza con l'intermediario resistente. Non è agli atti, tuttavia, la parte iniziale della conversazione in cui trarre eventuale conferma della ricostruzione della ricorrente; è invece stato prodotto lo stralcio nel quale il terzo chiede di inviare un'email a un indirizzo di posta elettronica certificata (che corrisponderebbe a quello dell' "ufficio legale carte") per far presente il problema e chiedere di essere ricontattata, indicando i dati identificativi della propria posizione e i propri recapiti telefonici.

Sulla base delle indicazioni ricevute, con mail inviata nello stesso giorno 05.04.2018, all'indirizzo PEC fornito tramite chat, la ricorrente forniva il proprio codice cliente e il proprio recapito telefonico.

In esito a tale iniziativa, riceveva un SMS da un numero che sarebbe il medesimo dal quale la ricorrente ha poi ricevuto i successivi SMS alert per le operazioni contestate.

Con la mail del 09.04.2018 la ricorrente inviava, come richiestole, copia della propria carta di credito attiva e copia della richiesta della carta aggiuntiva.

All'esito di questo intenso scambio di comunicazioni, il terzo, finalmente entrato in possesso dei dati relativi alla carta, avrebbe realizzato le operazioni fraudolente.

La ricorrente dichiarava di aver provveduto al blocco della carta subito dopo aver ricevuto i 2 SMS ALERT relativi ai pagamenti contestati di € 1.379,98 e di € 100,00, fornendo il codice blocco indicato dall'operatore della Banca.

L'intermediario riferisce che le operazioni sarebbero state autorizzate con il corretto inserimento di tutti i codici dispositivi, in osservanza del protocollo "Full 3D".

Invero, il richiamato protocollo prevede per l'autenticazione del titolare l'inserimento, al momento del perfezionamento dell'acquisto, di una password temporanea generalmente fornita a mezzo SMS: procedura che nel caso di specie, dal punto di vista dell'intermediario, è stata rispettata.

L'intermediario fornisce inoltre copia della normativa contrattuale che prevede per le carte di credito un plafond standard mensile fino a € 1.500,00.

Per le carte di credito il servizio di alerting è automatico. La ricorrente fornisce copia di 2 SMS ALERT e l'intermediario il relativo tracciato.

La giurisprudenza di questo Arbitro univocamente stabilisce come in casi siffatti la domanda non possa essere accolta. Per tutte, in un caso del tutto analogo, cfr. Collegio di Napoli - pronuncia n. 7634 del 28.6.2017, nel senso che "in conformità al consolidato orientamento di questo Arbitro sul tema, il comportamento del cliente risulta connotato da colpa grave, anche in relazione a quanto prescritto dal punto 2.1 sez. IV delle disposizioni della Banca d'Italia del 5 luglio 2011 "Attuazione del Titolo II del Decreto legislativo n. 11

del 27 gennaio 2010 relativo ai servizi di pagamento", secondo cui l'utilizzo di dispositivi personalizzati di sicurezza (es. PIN e password) obbliga l'utilizzatore a mettere in atto gli accorgimenti idonei al fine di preservarne la riservatezza, onde evitare gli utilizzi non autorizzati degli strumenti di pagamento in questione. Il cliente ha infatti fornito le proprie credenziali aderendo ad una sollecitazione che solo apparentemente proveniva dall'intermediario, senza rendersi conto che gli intermediari non inviano tali sollecitazioni… sicché si deve concludere che ricorra quella straordinaria ed inescusabile imprudenza e negligenza in presenza della quale le conseguenze del phishing non possono che ricadere sul cliente utilizzatore, dovendone al contrario rimanere estraneo l'intermediario (cfr. in senso conforme Collegio Napoli, decisione n. 997/2017 e n. 2188/2017)". Ed ancora, cfr. Collegio di Napoli - pronuncia n. 9343 del 20.10.2016, nel senso che "non può disconoscersi come il ricorrente abbia ammesso di avere "abboccato" ad un phishing, fornendo i propri dati in seguito alla richiesta delle credenziali, contenuto in un messaggio solo in apparenza proveniente dall'intermediario. Pertanto, si può qui ragionevolmente ravvisare una responsabilità del cliente – come tale rilevante ai sensi dell'art. 1227 c.c. – in relazione alla mancata diligente custodia dei codici d'accesso al servizio di home banking, dal momento che è opinione unanimemente condivisa, sulla base della disciplina vigente, che sul cliente gravi l'onere di custodire con la massima diligenza i vari codici in suo possesso, necessari per compiere operazioni bancarie di vario genere, siano esse prelievi per mezzo del servizio Bancomat come disposizioni di operazioni per mezzo di servizi on line".
Ne vi sono in atti evidenze differenti, circa la possibile provenienza dell'atto fraudolento da soggetti in qualche modo riferibili all'intermediario.
Il ricorso, alla luce di quanto esposto, e della giurisprudenza di questo Arbitro, che si condivide, non può essere accolto.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE LEONARDO CARRIERO