Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) ACHILLE	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) BARILLA'	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore (MI) TINA

Seduta del 09/11/2021

FATTO

In data 9.03.2021, il ricorrente tentava di accedere all'App dell'Intermediario resistente, ma riceveva un messaggio di "*negato accesso*"; successivamente, effettuava altri 3 tentativi con il medesimo esito per poi fermarsi (dal momento che, dopo il terzo tentativo, l'accesso sarebbe stato bloccato).
Poco dopo, riceveva un messaggio dal seguente tenore: "*Gentile cliente B** stiamo provvedendo a sospendere le sue utenze Bancarie per mancato aggiornamento per evitare Accedi. https://sicurezza-app-aggiorna.com*". Il ricorrente non utilizzava il link ricevuto. Contemporaneamente, riceveva una telefonata da un presunto operatore dell'Intermediario, che gli riferiva che, per sbloccare l'accesso dall'App, avrebbe dovuto ricevere una mail.
In seguito, durante un'altra telefonata gli veniva richiesto il numero della carta di credito per sbloccare l'accesso; il ricorrente forniva il dato richiesto, ma non il codice di sicurezza CVV della carta.
Su richiesta del ricorrente, l'operatore riferiva di essere a conoscenza del codice di accesso alla App, che, infatti, confermava correttamente. Nel frattempo, il ricorrente riceveva un'email dell'Intermediario resistente con cui gli veniva richiesto di cliccare su un link per ottenere i "codici di autenticazione"; il ricorrente ignorava anche questo link.
Dopo qualche ora, il ricorrente veniva informato tramite SMS dell'esecuzione di una operazione di pagamento con la propria carta credito per l'importo di Euro 2.950,00 e di altre tre operazioni effettuate con la carta bancomat; provvedeva, pertanto, a contattare

immediatamente il numero verde dell'Intermediario resistente, richiedendo il blocco delle due carte e l'accesso all'home banking.
L'Intermediario resistente ha stornato due dei tre pagamenti effettuati tramite POS (per l'importo di Euro 200,00 ed Euro 99,00), ma non la terza operazione per un importo di Euro 500,00 e quella eseguita con carta di credito (Euro 2.950,00).
Presentata denuncia-querela in data 10.03.2021 ed esaurita la fase di reclamo, con il ricorso all'ABF il ricorrente ha chiesto il rimborso degli importi corrispondenti alle operazioni non autorizzate, pari complessivamente a Euro 3.450,00.
Con le proprie controdeduzioni, l'Intermediario resistente ha precisato quanto segue:

- il cliente sarebbe stato vittima di phishing tramite *sms spoofing* e successivo *vishing;*
- il cliente avrebbe depositato integrazione della denuncia, dichiarando di non aver fornito – durante il dispiegarsi dell'iter criminoso - alcun codice o aperto alcun link, soltanto dopo 2 mesi;
- le operazioni fraudolente sarebbero state effettuate prima del blocco delle carte;
- in data 22.03.2021, il cliente avrebbe inviato reclamo formale all'intermediario dichiarando, in aggiunta a quanto rappresentato in denuncia, che il sedicente operatore lo avrebbe invitato a disinstallare l'App dell'intermediario "per far sì che potesse resettare e riattivare correttamente il tutto";
- il cliente avrebbe comunicato al sedicente operatore dell'intermediario i dati delle proprie carte e, presumibilmente, anche i codici di autenticazione (ID e password per accedere all'App), nonché il codice OTP con il quale i frodatori sarebbero riusciti ad installare l'App sul proprio smartphone;
- relativamente alle operazioni da Euro 200,00 ed Euro 99,00, l'intermediario dichiara di non aver effettuato alcun rimborso: esse sarebbero state spontaneamente stornate dall'esercente in seguito alla segnalazione di frode.

Con successive repliche, il ricorrente ha osservato quanto segue:

- che la ricostruzione operata nella denuncia non risponderebbe al vero (in ragione di un errore del verbalizzante): egli dichiara, accortosi di ciò, di aver chiesto agli operatori dell'intermediario se fosse necessario procedere ad una rettifica della denuncia, ma questi lo avrebbero rassicurato rappresentandogli che non fosse necessario;
- ha provveduto ad integrare la denuncia (con la precisazione di non aver mai comunicato dati riservati e sensibili delle carte) dopo aver realizzato che su tale aspetto si fosse imperniata la difesa dell'intermediario ed allega, a tal riguardo, la testimonianza di una persona presente durante la chiamata;
- se anche avesse provveduto a comunicare al malfattore il codice della carta di credito, non sarebbe possibile spiegare come fosse stato possibile per quest'ultimo disporre operazioni relative anche alla carta bancomat (che non disporrebbe di alcun codice segreto);
- diversamente da quanto sostenuto dall'intermediario, di non aver mai cliccato sui messaggi ricevuti (che non avrebbe neanche aperto);
- il sedicente operatore gli avrebbe comunicato telefonicamente il codice per l'accesso all'applicazione dell'intermediario senza che il cliente glielo avesse preventivamente riferito.

DIRITTO

La questione rimessa all'esame del Collegio riguarda l'esecuzione di due operazioni di pagamento effettuate con la carta di credito e con la carta bancomat del ricorrente per un importo complessivo di Euro 3.450,00. Il ricorrente riferisce, in sintesi, di essere rimasto vittima di un episodio di spoofing misto a vishing avvenuto in data 9.3.2021. Le operazioni contestate dalla ricorrente, avvenute nella medesima giornata, sono, quindi, assoggettate alle disposizioni del D.lgs. n. 11/2010 nella versione oggi vigente.
Ciò premesso, giova anzitutto precisare che, per l'ipotesi di disconoscimento di operazioni da parte del cliente, l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.
Nel caso di specie, per quanto attiene alla condotta tenuta dal ricorrente, questa appare certamente connotata da leggerezza per avere il ricorrente prestato fede a comunicazioni con profili di anomalie e aver comunicato le credenziali di sicurezza relative all'utilizzo dello strumento di pagamento. Da un lato, il messaggio ricevuto dal ricorrente risulta essere il primo e non in coda a precedenti messaggi genuini, presentando, inoltre, una forma lessicale non del tutto corretta; dall'altro lato, il link contenuto nello stesso messaggio non appare direttamente riconducibile all'intermediario resistente. Non si presenta pertanto quella aggressione informatica sofisticata propria dello spoofing, che consiste nella manipolazione dei dati relativi al mittente di un messaggio per far sì che esso appaia provenire da un soggetto differente, mediante la sostituzione del numero originario con un testo alfanumerico riconducibile a quello utilizzato dall'intermediario per i propri messaggi genuini.
Ciò nonostante, le richieste del ricorrente devono trovare accoglimento.
Occorre, infatti, evidenziare che nel caso di specie l'Intermediario resistente non ha fornito, come sarebbe stato suo onere, piena prova circa l'adozione di un sistema di autenticazione forte, con riferimento in particolare all'attivazione dell'App utilizzata per l'esecuzione delle operazioni disconosciute dal ricorrente tramite carta di credito e carta bancomat, in riferimento alla quale non risulta in atti alcuna documentazione di supporto.
Di conseguenza, anche sulla base di quanto previsto dall'art. 12, comma 2-*bis*, d.lgs. n. 11/2010 (secondo cui "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"), la ricorrente ha diritto ad ottenere il rimborso integrale dell'importo corrispondente alle operazioni fraudolente effettuate mediante la sua carta di pagamento, pari a Euro 3.450,00, oltre interessi dal reclamo al saldo.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 3.450,00.
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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE facente funzioni

Firmato digitalmente da
DAVIDE ACHILLE