Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore NICOLA RIZZO

Seduta del 17/09/2024

FATTO

La cliente, nel ricorso, afferma quanto segue: che, in data 15/02/2024, alle ore 20.10, riceveva una telefonata sul proprio cellulare dal numero 800***639, riconducibile al servizio clienti dell'intermediario e notoriamente attivo 24 ore su 24; che l'interlocutore si qualificava come operatore dell'intermediario e la informava che erano in corso tentativi di addebito sul suo conto, anche dall'estero, e che gli stessi erano monitorati da parte della banca perché considerati sospetti; che la cliente negava di aver eseguito i pagamenti in questione e il sedicente operatore le chiedeva se volesse procedere con il disconoscimento degli stessi; a tal fine, le chiedeva il codice fiscale e al contempo le forniva, evidentemente per rassicurarla, il numero della sua carta d'identità; che si era registrata, all'apertura del rapporto bancario, fornendo copia della propria patente di guida. A fronte della scadenza di questa in data 07/02/2024, la cliente aveva quindi provveduto nel gennaio 2024 a caricare online la propria carta d'identità elettronica, il cui numero era conosciuto dal falso operatore; comunicava dunque il dato richiesto, confidando nella genuinità della comunicazione sulla base di diverse circostanze: la telefonata proveniva dal numero del servizio clienti dell'intermediario, il sottofondo udibile al telefono era costituito da altre conversazioni similari, come se la chiamata provenisse da un centralino, l'interlocutore conosceva le sue generalità e il numero della sua carta d'identità, la richiesta del codice fiscale veniva solitamente attuata ad ogni contatto telefonico del

numero verde, l'intermediario opera esclusivamente online e dunque è necessario operare tramite computer o cellulare; che il presunto operatore la informava che le sarebbero arrivati dei messaggi, necessari per iniziare la procedura che solo il medesimo, con la collaborazione della cliente, avrebbe potuto eseguire per procedere allo storno dei pagamenti fraudolenti; che il primo messaggio, che la invitava ad eseguire le istruzioni dell'operatore, perveniva alle ore 20.14 e si collocava nella chat ufficiale dell'intermediario, così come tutti gli SMS successivi, rafforzando ulteriormente la convinzione della genuinità della telefonata; che il sedicente operatore comunicava che le operazioni avrebbero dovuto essere prima autorizzate e poi revocate, a tal fine chiedendo i codici temporanei che l'intermediario avrebbe inviato tramite SMS; che quando comunicava i codici all'interlocutore, comparivano sull'applicazione della banca, in alto sullo schermo del cellulare, anche le notifiche temporanee, riportanti prima la dicitura "pagamento accettato" e quindi "pagamento rifiutato"; che, nel corso della telefonata, la ricorrente riceveva anche 5 messaggi con i quali venivano inviate altrettante password per l'accesso; che, dopo 57 minuti di telefonata, l'operatore riferiva che, per problemi di sovraccarico delle linee del centralino, avrebbe dovuto contattarla da un'altra utenza.
Subito dopo, infatti, riceveva una telefonata dall'utenza 346***744, effettuata dal precedente interlocutore, nel corso della quale continuavano ad essere adottate le modalità operative già descritte; nel corso della chiamata, riceveva in totale 38 messaggi, tutti sulla chat della banca; alla fine della telefonata, l'operatore comunicava che era stato tutto risolto e che il suo account era stato temporaneamente bloccato per impedire che nel corso della notte ci fossero altri tentativi impropri di addebito; assicurava che la mattina dopo, tra le 8 e le 8.30, la stessa sarebbe stata richiamata dal servizio clienti per lo sblocco delle credenziali (e quindi per riattivare l'utenza).
Il giorno successivo, il 16/02/2024 alle ore 8.46, contattava il servizio clienti (ricevendo richiesta, da parte dell'operatore, della comunicazione del codice fiscale), al numero 800***639, e così si avvedeva di aver subito una truffa per l'importo di € 10.802,00; chiedeva all'operatore di bloccare il conto, la carta di debito e le operazioni fraudolente, soprattutto con riferimento ai bonifici bancari, attesa la loro esecuzione solo poche ore prima; si recava in questura per presentare denuncia, ma in questa sede le veniva riferito che era necessario l'estratto conto attestante i movimenti contestati: chiamava quindi più volte il numero verde dell'intermediario nei giorni 16 e 17/02/2024 per farsi inviare l'estratto conto, ma senza ottenerlo, nonostante le fosse assicurato che si stava provvedendo; lunedì 19/02/2024 si recava nuovamente in questura, ottenendo la possibilità di dar comunque corso alla denuncia.
Presentava reclamo all'intermediario, che veniva riscontrato negativamente; contesta che l'intermediario non ha provato la circostanza che tutte le operazioni risultino essere state correttamente disposte con autenticazione forte del cliente; che l'intermediario è venuto meno agli obblighi di protezione che discendono dalle norme di diritto comune; che, visto il numero delle operazioni e la brevissima distanza temporale tra queste, è stato superato il rischio frode di cui all'art. 8 del D.M. n. 112/2007; che, con riferimento ai bonifici, quello dell'importo di € 4.850,00 risulta essere stato eseguito in data 16/02/2024, giorno in cui la banca era venuta a conoscenza, fin dalle ore 8.46, della frode; inoltre l'intermediario ha lasciato colpevolmente trascorrere un considerevole lasso di tempo prima di richiamare il bonifico.
La ricorrente domanda, quindi, il rimborso della somma complessiva di euro € 10.802,00.
L'intermediario convenuto, riportato il fatto, afferma quanto segue: che le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; che sussiste la colpa grave della cliente, in considerazione della mole dei contatti intercorsi con i terzi malfattori e dei codici condivisi

con questi ultimi, nonché del tempo intercorso tra l'esecuzione della prima e dell'ultima operazione; che la banca mette a disposizione dei propri clienti numerosi contenuti in materia di sicurezza informatica, ivi incluso un contenuto dedicato alle frodi perpetrate mediante la tecnica del c.d. vishing; che gli SMS contenenti le OTP riportavano con chiarezza la finalità di utilizzo di ciascun codice ed avvisavano che l'intermediario non avrebbe mai chiesto tali codici: se la cliente avesse ricevuto tale richiesta, si sarebbe trattato di una frode; che la banca ha informato la cliente in tempo reale di tutte le azioni poste in essere, mediante comunicazioni trasmesse via email e notifiche push: anziché leggere attentamente ciascuna notifica, questa ne ignorava il contenuto; che la banca ha in ogni modo tentato di proteggere l'area riservata della cliente, provvedendo a bloccarne l'accesso numerose volte, ma questa agevolava in maniera gravemente colposa l'esecuzione delle operazioni disconosciute (poche, rispetto a tutte quelle disposte dai terzi e bloccate proprio grazie agli interventi dell'intermediario).
L'intermediario convenuto domanda, pertanto, il rigetto del ricorso in quanto infondato in fatto e in diritto.

DIRITTO

Oggetto della presente controversia sono nove operazioni, per un importo complessivo di € 10.802,00, poste in essere il 15 e il 16 febbraio 2024.
Alla data delle operazioni trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.
È in atti la denuncia della cliente presentata in data 19/02/2024 e la relativa integrazione del 23/02/2024.
Relativamente all'autenticazione forte con riferimento alle fasi antecedenti all'esecuzione delle operazioni contestate, dalla ricostruzione fornita dall'intermediario e dalla documentazione prodotta si evince che, in data 15/02/2024 alle ore 20.27, un soggetto collegato all'area personale tramite "Web Desktop" abbia avviato la procedura di modifica della password, utilizzando come fattori di autenticazione: username e due cifre del PIN della carta di debito collegata al conto corrente (fattore di conoscenza); SMS OTP (fattore di possesso). L'intermediario fa coincidere tale operazione con il login preliminare alla esecuzione della prima delle operazioni contestate. Si tratterebbe, in altri termini, di un accesso realizzato con la procedura prevista per il caso di sblocco dell'account o di password dimenticata.
Osserva questo Collegio che la documentazione prodotta evidenzia un "Login GT" alle ore 20.28 del 15/02/2024, subito dopo la modifica della password, realizzato utilizzando la password personale (cfr. Allegato 2 alle ctd, riga 84, colonna "Medio de autentificación" = "Autenticación con usuario y password personales"), dunque un fattore di conoscenza. Nulla si desume in merito a un secondo fattore.
Questo profilo è stato valorizzato di recente dal Collegio di Milano (cfr. decisione n. 8781/24 del 25/07/2024) che ha ritenuto, in una fattispecie del tutto analoga, non provata la SCA.
Il medesimo difetto di prova dell'autenticazione forte si constata, peraltro, anche nella fase esecutiva delle operazioni contestate.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 10.802,00.
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

Firmato digitalmente da
FLAVIO LAPERTOSA