COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) COSTA	Membro di designazione rappresentativa dei clienti

Relatore FEDERICA COSTA

Seduta del 20/05/2025

FATTO

Con ricorso presentato il 30.10.2024 la ricorrente riferisce di essere titolare di un conto corrente presso l'intermediario resistente ed abilitato al servizio di internet banking. In data 23 febbraio 2024, alle ore 21:19, riceveva sul proprio telefono cellulare un messaggio SMS, apparentemente proveniente da un numero di telefonia mobile, nel quale veniva segnalato un presunto tentativo di prelievo anomalo, effettuato dalla città di Lugano. Preoccupato della notizia e ritenendola attendibile, il ricorrente accedeva al link indicato nel messaggio, ritrovandosi su una pagina web che riproduceva fedelmente l'interfaccia grafica dell'home banking dell'intermediario. All'interno di tale sito venivano richiesti il nome, il cognome e il numero di telefono del cliente, dati che egli forniva senza tuttavia dover inserire alcuna credenziale di accesso riservata. Successivamente, nell'arco di circa mezz'ora, il ricorrente riceveva due telefonate da un numero fisso; l'interlocutore, qualificatosi come operatore dell'intermediario, lo rassicurava che le attività sospette erano sotto controllo e lo invitava a disconoscere il pagamento riferito a Lugano, raccomandandogli altresì di non accedere all'home banking, in quanto – a suo dire – il portale era in fase di blocco tecnico. Venivano quindi eseguiti ben ventidue bonifici non autorizzati, per un ammontare complessivo pari a € 54.970,00. Resosi conto dell'accaduto, il ricorrente sporgeva tempestiva denuncia presso l'autorità competente, segnalando altresì che anche un secondo conto corrente – intestato alla ditta individuale

della propria coniuge – era stato oggetto di due ulteriori disposizioni fraudolente per € 4.990,00. Soltanto una parte della somma sottratta, pari a € 10.000,00, veniva successivamente recuperata e riaccreditata dall'intermediario mediante i circuiti bancari, mentre il rimborso del restante importo veniva negato. Il ricorrente chiede il "*riaccredito delle somme, distolte con frode, sul conto corrente…della società ricorrente*".

L'intermediario convenuto, nelle proprie controdeduzioni dd. 22.01.2025, conferma l'avvenuto recupero della somma di € 10.000,00, che veniva riaccreditata sul conto della cliente in data 21 marzo 2024, evidenziando tuttavia come la pretesa azionata debba intendersi oggi limitata all'importo residuo di € 44.970,00. Sottolinea che l'accesso all'area riservata del servizio di internet banking risulta subordinato all'inserimento di credenziali statiche (Codice Titolare e PIN) e all'impiego di una password dinamica (codice OTP) generata tramite sistema di Firma Digitale Remota (FMV), in uso esclusivo del cliente. Secondo la ricostruzione dell'intermediario, tutte le operazioni contestate sono state regolarmente registrate e tracciate dai sistemi informatici, senza che siano emerse anomalie o malfunzionamenti tecnici. I dati di accesso risultano associati all'utenza telefonica intestata alla ricorrente. In particolare, nella serata del 23 febbraio 2024, alle ore 21:41:13, veniva effettuato l'enrollment di un nuovo dispositivo mobile all'home banking del cliente, previa digitazione del Codice Titolare, del PIN e del codice OTS (One Time Setup), inviato via SMS al numero certificato.

Tale operazione, secondo l'intermediario, costituisce la premessa indispensabile per poter disporre transazioni dispositive, tutte avvenute tra le ore 21:48 del 23 febbraio e le ore 12:03 del 24 febbraio. La responsabilità dell'accaduto, a parere del convenuto, ricade interamente sul cliente, che avrebbe mostrato un comportamento gravemente negligente, accedendo a un link sospetto e aderendo alle istruzioni impartite telefonicamente da un soggetto terzo, non identificato, senza verificare l'autenticità della comunicazione. Il messaggio SMS contenente il codice OTS, inoltre, riportava in modo esplicito l'indicazione di non condividerlo con terzi: circostanza che sarebbe stata ignorata, come dimostra la coincidenza temporale tra la chiamata telefonica e la ricezione del codice stesso. Chiede quindi il rigetto del ricorso avversario.

Con repliche dd. 7.1.2025 la ricorrente contesta le argomentazioni dell'intermediario, negando di aver mai comunicato a terzi le proprie credenziali di accesso, né quelle statiche né quelle dinamiche. Ribadisce di essere stata vittima di un sofisticato attacco informatico, il quale si è avvalso di tecniche di spoofing tali da ingannare anche un utente accorto. A suo avviso, l'intermediario non avrebbe approntato misure di sicurezza adeguate a contrastare minacce tanto evolute, omettendo di attivare sistemi di allerta automatica o di blocco, nonostante la sequenza delle operazioni fraudolente si sia protratta per oltre dodici ore. Il ricorrente aggiunge che nella mattinata del 24 febbraio, attorno alle ore 9:00, un funzionario dell'intermediario lo contattava telefonicamente per segnalare genericamente "movimenti sospetti", senza tuttavia procedere al blocco delle successive disposizioni, che proseguirono fino alle ore 12:03. Inoltre, rileva come il numero verde dell'intermediario, dedicato ai clienti imprese, fosse irraggiungibile nel fine settimana, a partire dal pomeriggio del venerdì.

Con controreplica dd. 22.01.2025, l'intermediario insiste sulla piena riconducibilità delle operazioni al cliente, sottolineando che il messaggio fraudolento era inviato da un numero mobile privo di riferimenti ufficiali e contenente errori sintattici e link non appartenenti al dominio della banca. Ritiene che *l'enrollment* del dispositivo e la successiva operatività dispositiva siano state possibili solo grazie alla collaborazione, anche se inconsapevole, del cliente, il quale avrebbe comunicato il codice OTS ricevuto via SMS, nonostante

l'avvertenza espressa di non condividerlo. Precisa, inoltre, che il cliente contattava la filiale online solo alle ore 14:14 del 24 febbraio, ottenendo il blocco dell'home banking alle ore 14:20, quando ormai le operazioni risultavano eseguite. Sottolinea infine che le disposizioni in questione presentavano un'apparenza di regolarità, potendo essere interpretate – per entità e periodicità – come pagamenti di tipo aziendale (quali, ad esempio, il versamento di stipendi), e che, in assenza di elementi oggettivi di anomalia, l'intermediario era tenuto ad eseguire le disposizioni impartite in conformità agli obblighi contrattuali vigenti.

Il Collegio nella riunione del 18 marzo 2025 ha deliberato di "*invitare l'intermediario a indicare quali siano le operazioni per le quali la procedura di recall ha avuto esito positivo*".

Con nota del 27 marzo 2024 l'intermediario ha riscontrato la richiesta di integrazione e ha precisato che le operazioni per le quali la procedura di recall ha avuto esito positivo sono n. 4 bonifici effettuati il 24.02.2024 dalle ore 10:13, alle ore 10:17, alle ore 10:18 e alle ore 10:20.

DIRITTO

Parte ricorrente lamenta l'esecuzione fraudolenta di n. 22 bonifici non autorizzati, effettuati tra le ore 21:48 del 23 febbraio 2024 e le ore 12:03 del giorno successivo, per un importo complessivo pari ad € 54.970,00 (cfr. distinta bonifici prodotta dall'intermediario). Il blocco dell'operatività dell'home banking è stato disposto soltanto alle ore 14:20 del 24 febbraio. A fronte dell'attivazione della procedura di "recall", l'intermediario riusciva a recuperare soltanto € 10.000,00, accreditati sul conto del ricorrente in data 21 marzo 2024. Ne consegue che l'importo residuo oggetto di richiesta giudiziale è pari ad € 44.970,00.

La controversia verte sulla ripartizione del rischio in caso di operazioni di pagamento non autorizzate, per come disciplinata dagli articoli 10, 11 e 12 del D.lgs. n. 11/2010. Ai sensi dell'art. 10, comma 1, il prestatore di servizi di pagamento è tenuto a garantire che ogni operazione di pagamento sia eseguita soltanto previa autenticazione forte del cliente, ove prevista, e, in ogni caso, solo con il consenso espresso di quest'ultimo. Qualora l'utente contesti l'autenticità dell'operazione, l'onere della prova circa la corretta autenticazione della stessa, nonché della sua riconducibilità all'utente, grava sull'intermediario (art. 10, comma 2).

L'art. 12, comma 1 dispone che, in caso di operazione di pagamento non autorizzata, il prestatore dei servizi di pagamento rimborsa al pagatore l'importo dell'operazione immediatamente, e comunque non oltre la fine della giornata lavorativa successiva alla contestazione.

È solo in caso di dolo o colpa grave dell'utente che questi può essere ritenuto responsabile delle perdite subite (art. 12, comma 3). Tale valutazione deve essere operata secondo criteri rigorosi e oggettivi, come affermato dalla costante giurisprudenza dell'ABF (Collegio Bologna, n. 4737/24).

Nel caso in esame, i 22 bonifici oggetto di contestazione: - sono stati eseguiti in un lasso temporale ristretto (meno di 15 ore); - sono accomunati da importi omogenei (20 operazioni da € 2.500,00; 2 da € 2.490,00 e € 2.480,00); - risultano in parte indirizzati a medesimi beneficiari con rapidissima successione temporale. Tali circostanze appaiono

oggettivamente anomale, anche alla luce dei parametri di rischio indicati dal D.M. 30 aprile 2007, n. 112, in particolare l'art. 8, lett. a), punto 2, che prevede l'esistenza di rischio di frode qualora vi siano "*tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita*". Pur trattandosi di bonifici e non di transazioni su POS, l'ABF ha più volte chiarito l'applicabilità analogica di tali indici sintomatici di rischio, ogniqualvolta ricorra una evidente anomalia rispetto all'operatività storica dell'utente (cfr. ABF, Collegio Milano, n. 20530/2020; Bologna, n. 18713/2021; Torino, n. 3464/2018). Inoltre, l'assenza di blocco automatico delle operazioni successive all'avviso di attività sospette (comunicato dallo stesso intermediario nella mattina del 24 febbraio) suggerisce un difetto di presidio tecnico o una inadeguatezza nei sistemi di monitoraggio antifrode.

In ordine alla condotta dell'utente, non risultano atti di condivisione consapevole delle credenziali di accesso: il link malevolo e l'interfaccia simulata, nonché le telefonate manipolative, costituiscono condotte di terzi qualificabili come phishing. La ricorrenza di tali modalità di truffa, pur non escludendo in astratto la colpa grave, impone un'analisi rigorosa e caso per caso, tenendo conto anche delle misure predisposte dall'intermediario per contenerne gli effetti.

Al riguardo, il Collegio osserva che le parti non hanno fornito alcuna informazione circa il sistema di alert. Nel caso in esame, dunque, non risultano informazioni sull'invio e la ricezione di notifiche di alert da parte dell'intermediario al cliente. Il Collegio rileva che, poiché i 22 bonifici sono stati eseguiti in un lasso temporale di circa 15 ore, l'intermediario non ha diligentemente monitorato né avvisato il cliente delle operazioni in corso, che risultano in parte indirizzate a medesimi beneficiari con una rapidissima successione temporale e che, pertanto, non potevano essere ricondotte a versamenti di stipendi, come sostenuto dalla parte resistente.

Nel caso di specie, applicando l'indicatore di anomalia di cui all'art. 8, lett. a), punto 2 del D.M. 112/2017, il Collegio dichiara l'intermediario tenuto a rimborsare i bonifici dal terzo compreso in poi (con l'unica eccezione dei n. 4 bonifici per i quali la procedura di recall ha avuto esito positivo, i.e. quelli effettuati il 24.02.2024 dalle ore 10:13, alle ore 10:17, alle ore 10:18 e alle ore 10:20).

PER QUESTI MOTIVI

Il Collegio – in parziale accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 39.980,00 (trentanovemilanovecentottanta/00).
Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
CHIARA TENELLA SILLANI