COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) VARDI	Membro di designazione rappresentativa dei clienti

Relatore - FABRIZIO MAIMERI

Seduta del 10/07/2025

FATTO

Con ricorso del 4.11.2024, parte attrice riferisce che il 23.2.2024 una propria dipendente, che aveva accesso e gestiva in prima persona i conti della società ricorrente, riceveva un *sms* apparentemente proveniente dalla Banca resistente, con il quale veniva notificata un'operazione di pagamento di € 875,00. Il messaggio conteneva un *link* al quale la dipendente accedeva senza fornire dati sensibili, credendo di bloccare il pagamento. Il giorno successivo riceveva una chiamata da un numero riconducibile alla banca, nel corso della quale un sedicente operatore le suggeriva di collegarsi al sito *infobiz.com* e di accedere al conto corrente; allertata dalla natura insolita della procedura, essa provava a mettersi in contatto con il servizio clienti della banca, senza successo. Si scopriva solo in un secondo momento che, tra le 12.52 e le 13.12, erano stati effettuati 8 bonifici di € 2.500,00 ciascuno a valere sul conto della società. A seguito del disconoscimento veniva recuperata la somma di € 4.900,00. La società ricorrente sottolinea che le operazioni sono state effettuate di sabato e sostiene che il servizio clienti non fosse attivo; contesta pertanto alla banca di non aver consentito il tempestivo blocco del conto. Chiede il rimborso di € 15.100,00.

In sede di controdeduzioni, l'intermediario premette che, a seguito del disconoscimento delle operazioni, sono stati recuperati tramite il circuito interbancario € 4.900,00, onde

l'importo oggetto del contendere è di € 15.100,00. Afferma che le operazioni contestate sono state regolarmente autorizzate registrate e contabilizzate. A questo proposito precisa che, per accedere ai servizi *online*, è necessario utilizzare codice titolare, codice PIN e OTP. L'OTP è generata da *app* attraverso la digitazione del PIN oppure, per i clienti che non utilizzano il sistema *O-*** smart*, via *sms*. Nel caso di specie, le transazioni sono state autorizzate attraverso l'*app* installata sul dispositivo del truffatore. L'*enrollment* dell'*app* su tale dispositivo è avvenuta il 24.2.2024 alle 12.13, tramite codice titolare, PIN e OTP trasmesso via *sms*. A seguito della attivazione dell'*app*, è stato effettuato l'accesso al conto e sono stati disposti gli otto bonifici di € 2.500,00, rispettivamente alle 12.52, 13.01, 13.05, 13.06, 13.07, 13.09, 13.10, 13.12. Tutte le operazioni sono state autorizzate con OTP generata da *app* a seguito della digitazione del PIN. Tali operazioni sono imputabili alla negligente custodia dello strumento di pagamento e delle relative credenziali da parte dell'utente. Nel dettaglio, la dipendente della società ha interagito con un *link* truffaldino, ha dato credito alle indicazioni ricevute telefonicamente da un falso operatore del servizio clienti e ha comunicato a quest'ultimo le credenziali bancarie, come dichiarato anche nel modulo di disconoscimento. Peraltro, la società ricorrente non produce copia della *chat* telefonica o del registro chiamate. Alla luce di quanto precede, la Banca chiede il rigetto del ricorso o in subordine la ripartizione delle responsabilità secondo il disposto dell'art. 1227 c.c.

In sede di repliche, la ricorrente contesta alla Banca di non aver fornito prova della corretta autenticazione delle operazioni e della colpa grave dell'utente. A questo proposito ribadisce di essere rimasta vittima di una frode sofisticata. Nega di aver comunicato dati personali a terzi. Ribadisce di non essere riuscita, nell'arco delle tre ore successive alla chiamata truffaldina, a mettersi in contatto con il servizio clienti della Banca. Contesta l'inefficienza dei presidi di sicurezza dell'intermediario. Sostiene inoltre che l'intermediario avrebbe dovuto effettuare controlli più stringenti sulle operazioni e sospendere immediatamente l'operatività del conto. Insiste, in conclusione, per l'accoglimento integrale del ricorso e, in subordine, per la ripartizione delle responsabilità almeno nella misura di 2/3 a carico della Banca.

In sede di controrepliche, la Banca ribadisce che le operazioni disconosciute sono imputabili alla negligente condotta dell'utente. Evidenzia che il *link* civetta non contiene riferimenti alla banca e che nel modulo di disconoscimento la dipendente della società ha dichiarato di aver comunicato i codici a terzi. Insiste per il rigetto del ricorso per le motivazioni già espresse nelle controdeduzioni.

In relazione alle rispettive argomentazioni, la ricorrente chiede all'Arbitro il «rimborso della somma di € 15.100,00». L'intermediario chiede al Collegio «a) [di] dichiarare inaccoglibile, in quanto immotivata ed infondata, la richiesta restitutoria oggetto del ricorso presentato [dalla ricorrente]; b) nella denegata ipotesi che il Collegio ritenga di poter ravvisare profili di responsabilità nell'accaduto in capo [all'intermediario], definire la ripartizione fra le parti del danno in esame, in misura proporzionale alle rispettive effettive responsabilità ed in particolare ai sensi dell'art. 1277, 1 e 2 comma c.c. con l'applicazione della franchigia di € 50,00 contemplata dalla normativa in materia di servizi di pagamento».

DIRITTO

La controversia ha ad oggetto 8 operazioni di bonifico istantaneo di € 2.500,00 ciascuna, effettuate il 24.2.2024 tra le 12.52 e le 13.12, a valere sul conto intestato alla società ricorrente. A seguito del disconoscimento sono stati recuperati € 4.900,00, sicché l'importo oggetto del contendere è di € 15.100,00.

In ordine alla sussistenza della SCA, l'intermediario riferisce che le operazioni disconosciute sono state eseguite dopo essere state autenticate, correttamente registrate e contabilizzate e non hanno subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o di altri inconvenienti. In dettaglio afferma che per accedere ai servizi *online* della Banca è richiesto l'inserimento:

(i) di due *password* statiche: il codice Titolare e il codice PIN;

(ii) una *password* dinamica: il codice *O-K*** (OTP).

Per autorizzare le operazioni dispositive è necessario il codice dinamico OTP, generato previa validazione della *push* trasmessa in app (*O-K*** *S****) o via *sms*, inviato sul numero di telefono certificato (*O-K***S***).

Quanto all'attivazione del *mobile token* su diverso dispositivo, dai *log* prodotti emerge che il *mobile token* è stato attivato mediante corretto inserimento del PIN [fattore di conoscenza] e del codice inviato al numero di telefono certificato del cliente [fattore di possesso]; gli stessi *log* prodotti contengono evidenza dell'invio del codice dinamico necessario per attivare il *mobile token*, trasmesso via *sms*.

Quanto alle 8 operazioni di bonifico istantaneo, esse sono state predisposte in *app* e autorizzate tramite PIN [fattore di conoscenza] che ha generato la OTP silente [fattore di possesso]. La modalità autorizzativa che viene in rilievo nel caso di specie utilizza una *token app* per la generazione di una OTP non visibile all'utente (sistema *O**** *S*****). Il Collegio di Roma ha ritenuto *compliant* alla SCA tale modalità autorizzativa: cfr. decisione n. 8530/2021, secondo cui «va (…) rilevato che il sistema di autenticazione messo a disposizione dall'intermediario risulta conforme ai requisiti della *Strong Customer Authentication* prescritti dalla PSD2 così come interpretati dall'EBA con l'"*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*" e ciò assume rilevanza cruciale in quanto, a fronte della disposizione di un'operazione di pagamento *on line* (art. 10 *bis*, comma 1, lett. b, d.lgs. n. 11/2010), il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte, salvo il caso in cui abbia agito in modo fraudolento (art. 12,comma 2-*bis*, d.lgs. n. 11/2010). Nel caso di specie risulta che per l'accesso al portale di *internet banking* sia necessario inserire un codice titolare, un PIN e un codice *O-K***, quest'ultimo generato da dispositivo *O-K** s******, ovvero da una *app mobile* per la generazione di codici OTP; per l'esecuzione delle operazioni dispositive; poi, sia necessario effettuare l'accesso al portale con le credenziali sopra indicate e autorizzare l'operazione mediante inserimento di codice OTP e, nel caso di operazioni valutate come sospette dal sistema antifrode, di un ulteriore codice OTS inviato al numero di cellulare certificato dell'utilizzatore. I *file* di tracciatura prodotti dalla resistente sembrano confermare quanto sopra».

Circa gli elementi rilevanti del fatto truffaldino, occorre rilevare che né il massaggio-civetta, né la *chat* sono state prodotte in atti. Da verifiche *online* risulta che il numero di provenienza della chiamata è associato a una filiale della banca resistente.

Si rammenta altresì che siffatta truffa integra il *vishing callerID*, fattispecie di frode insidiosa, quale ad esempio lo *spoofing*, che individua di solito un concorso colposo delle parti. In particolare, imputano alla banca la colpa poiché deve addossarsi sull'intermediario il rischio d'impresa relativo alla modalità di comunicazione adottata, propedeutica rispetto all'operazioni di disposizioni poi avvenute. «La frode, così congegnata, non sembra in effetti differire in maniera significativa dalle ipotesi di *spoofing*", ossia dalle ipotesi di *smishing* in cui il messaggio "esca" reca, quale mittente, la denominazione

dell'intermediario, in modo tale che il testo si inserisca, nei moderni smartphone, all'interno della conversazione contenente messaggi genuini (effettivamente provenienti dall'intermediario). E, secondo la più recente posizione condivisa dai Collegi territoriali dell'ABF, nelle fattispecie di *spoofing* è al più ravvisabile "un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di *phishing* e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario" (in questi termini v., per esempio, Collegio di Roma, decisione n. 1625/2022). Tenuto conto di tutti suddetti elementi di fatto e delle previsioni richiamate del d.lgs. n. 11 del 2010, il Collegio accerta una responsabilità dell'intermediario resistente, in concorso con il comportamento gravemente negligente della cliente, per i danni derivanti dal compimento dell'operazione di pagamento non autorizzata e dispone che l'intermediario corrisponda alla parte ricorrente l'importo di (…), a titolo di risarcimento del danno determinato in via equitativa»: così Collegio di Roma, decisione n. 8749/2024; nello stesso senso, Collegio di Milano, decisione n. 17467/2021.

Nell'ambito di queste considerazioni, va rimarcato che, nel caso di specie, sono state autorizzate 8 operazioni nell'arco di circa dieci minuti; gli 8 bonifici sono indirizzati verso 3 beneficiari (nel dettaglio uno dei beneficiari ha ricevuto due bonifici e gli altri due beneficiari hanno ricevuto 3 bonifici ciascuno). Inoltre, le operazioni sono state poste in essere in rapida successione temporale e per il medesimo importo. Sembrerebbero quindi tecnicamente ricorrere due indici di frode di cui all'art. 8, segnatamente: (a) comma 1, lett. b) del d.m. 30.4.2007, n. 112, ossia «1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento»; (b) comma 1, punto 2 della lett. a) dell'art. 8 d.m. n. 112/2007, ossia «tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore presso un medesimo punto vendita». Tuttavia, secondo l'orientamento dei Collegi, i principi del d.m. n. 112/2007 non hanno un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate ma sono espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'intermediario; sebbene tale decreto faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, gli indici di frode ivi disciplinati possono costituire un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o ricariche *online* o similari) in ragione dell'unicità della *ratio* sottesa a tale normativa; è inoltre possibile, sempre secondo l'orientamento dei Collegi, dare rilievo a indici di anomalia differenti da quelli tipizzati nel suddetto d.m. In conclusione, sulla falsariga di quanto normativamente indicato, i principi di correttezza e diligenza da rispettare nell'espletamento dell'attività bancaria spingono ad immaginare un comportamento dell'intermediario più attento nella protezione degli interessi del cliente, in fattispecie come quella in esame.

In relazione a quanto fin qui esposto, il Collegio ritiene che ricorrano gli estremi per un concorso di colpa fra le parti ai sensi dell'art. 1227 c.c. e di conseguenza, accogliendo parzialmente la domanda, accerta il diritto della società ricorrente a vedersi corrispondere dall'intermediario l'importo di € 6.500,00, calcolato in misura equitativa.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 6.500,00, determinata in via equitativa. 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
PIETRO SIRENA