COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) CARATOZZOLO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) CATTALANO	Membro di designazione rappresentativa dei clienti

Relatore GIUSEPPE SPENNACCHIO

Seduta del 28/05/2025

FATTO

Con ricorso in data 21 febbraio 2025 la ricorrente, titolare di un conto corrente intrattenuto con l'intermediario, riferisce che in data 3 febbraio 2025, alle ore 14.51, riceveva un messaggio da un identificativo riconducibile all'intermediario resistente. Deduce che, a questo punto, effettuava una telefonata al numero indicato dall'intermediario, chiedendo delucidazioni al riguardo.
Prosegue la narrazione affermando che alle 15.31 riceveva una nuova chiamata da un altro numero e da un diverso interlocutore, che le chiedeva di comunicare i codici nel frattempo giuntile via sms e via e-mail per completare, a suo dire, la procedura di riassociazione del suo dispositivo. Riferisce di avere in seguito letto un'e-mail dell'intermediario contenente l'avvertimento che il precedente dispositivo non era più associato al conto e che era stato associato un nuovo dispositivo, recante caratteristiche diverse da quello in proprio possesso.
Precisa che, dopo avere seguito le istruzioni impartitele, si avvedeva di un'operazione di prelievo fraudolento di €. 900,00= sul suo conto, che provvedeva a disconoscere. Tanto premesso, deduce che l'intermediario è responsabile in quanto le criticità nei sistemi di sicurezza del medesimo avrebbero consentito al truffatore di accedere ai suoi dati personali, consentendogli di portare a termine la frode.

La ricorrente chiede, quindi, all'Arbitro la restituzione della somma fraudolentemente sottrattale.
Costituitosi nel presente procedimento, l'intermediario deduce che, secondo la ricostruzione della ricorrente, quest'ultima ha seguito pedissequamente le istruzioni impartite dal sedicente operatore, consentendo che si perpetrasse una truffa attuata con le note tecniche del *phishing* e del *vishing*. Precisa che, dall'istruttoria effettuata a seguito della contestazione della ricorrente, sarebbe emerso che l'operazione oggetto del presente procedimento è stata eseguita tramite autenticazione forte, che le verifiche avrebbero accertato la totale assenza di fenomeni di malfunzionamento dei propri sistemi e che la condotta della ricorrente sarebbe connotata da colpa grave, perché non avrebbe dovuto fornire i propri dati di accesso al conto e perché, prestando attenzione alle chiamate del truffatore, avrebbe potuto impedire il perpetrarsi della truffa.
In particolare, evidenzia che il sedicente operatore è stato contattato dalla ricorrente su un'utenza mobile a sé non riconducibile e che gli ha fornito tutti i codici OTP pervenuti tramite sms, così consentendo al truffatore l'accesso all'*home banking* e l'associazione di un nuovo dispositivo. Per l'autorizzazione dell'operazione rinvia ai *log* allegati, rilevando che la ricorrente ha ricevuto un *alert* tramite notifica *push*.
Quanto alla colpa grave da imputare alla ricorrente evidenzia che quest'ultima ha seguito pedissequamente le istruzioni del truffatore. Chiarisce di avere reso edotta la propria clientela delle truffe ai danni degli utenti degli strumenti di pagamento tramite più canali e di avere inviato plurime e-mail sul tema all'indirizzo comunicato dalla ricorrente.
Quanto alle contestazioni relative alla pretesa inosservanza degli obblighi di protezione del cliente a carico dell'intermediario, rileva che i messaggi ricevuti dalla ricorrente durante la truffa indicavano chiaramente l'azione che si stava compiendo ("*stai richiedendo l'associazione di un nuovo dispositivo al tuo account*") e recavano altresì un monito sulla diffusione di quanto in essi contenuto. Insiste, quindi, per il rigetto del ricorso.

DIRITTO

Il Collegio rileva, in primo luogo, che l'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 che ha recepito la direttiva (UE) n. 2015/2366, relativa ai servizi di pagamento nel mercato interno, entrato in vigore il 13 gennaio 2018. Con riguardo a detta disciplina, il Collegio rammenta che, ai sensi dell'art. 10, d.lgs. n. 11/2010, "*Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento 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*".
Il secondo comma del medesimo art. 10 precisa, inoltre, che ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, "*l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7*" (obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Sempre il secondo comma stabilisce che "*è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente*".

La disciplina relativa all'autenticazione ed alle misure di sicurezza da adottare nel caso di operazioni elettroniche di pagamento a distanza è contenuta nell'art. 10-*bis*, d.lgs. n. 11/2010, secondo il quale "*i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente:*
a) accede al suo conto di pagamento on-line;
b) dispone un'operazione di pagamento elettronico;
c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.
Nel caso dell'avvio di un'operazione di pagamento elettronico di cui al paragrafo 1, lettera b), per le operazioni di pagamento elettronico a distanza, l'autenticazione forte del cliente applicata dai prestatori di servizi di pagamento comprende elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico".
Ai sensi dell'art. 1, comma 1, lett. q-*bis*, d.lgs. n. 11/2010, per "*autenticazione forte del cliente*" si intende "*un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione*".
Il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce un regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema. Il menzionato orientamento ha trovato riscontro nella giurisprudenza di legittimità, secondo cui la disciplina speciale relativa agli strumenti di pagamento ha esplicitato un principio generale applicabile in tema di onere probatorio a carico del debitore professionale nelle azioni di risoluzione contrattuale, risarcimento del danno o adempimento, in quanto si è ritenuto che non può essere omessa la verifica dell'adozione, da parte dell'istituto bancario, delle misure idonee a garantire la sicurezza del servizio; infatti, la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo, quindi, come parametro la figura dell'accorto banchiere: al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo.
Tanto premesso in termini generali, in ossequio ai principi in tema di riparto dell'onere probatorio sopra enucleati, è necessario innanzitutto verificare la conformità delle operazioni disconosciute alle prescrizioni normative in tema di SCA. Al riguardo, il Collegio osserva che l'intermediario ha fornito prova delle seguenti circostanze:
- alle ore 15.40 del 3 febbraio 2025 è stato effettuato, da un nuovo dispositivo, accesso all'*home banking* della ricorrente, attraverso due diversi *step* di autenticazione: il primo, mediante inserimento di *username* e *password* della ricorrente; il secondo, mediante inserimento di un codice OTP, inviato via sms al numero di cellulare della ricorrente con il seguente messaggio: "*Non comunicare a nessuno questo codice, inseriscilo nella app da cui stai eseguendo l'autenticazione*";

- una volta autenticato il nuovo dispositivo, questo è stato abilitato ad operare sul conto mediante inserimento nell'apposito campo di un ulteriore codice OTP, inviato via sms al numero di cellulare di cui sopra, con il seguente messaggio: "*Non comunicare questo codice a nessuno*";
- alle 15.45, dal nuovo dispositivo associato è stata eseguita l'operazione contestata.

Sulla base delle evidenze documentali versate in atti dall'intermediario, il Collegio, in conformità con il proprio precedente orientamento, conclude che il sistema di pagamento predisposto dall'intermediario ed utilizzato per il *login*, l'*enrollment* del nuovo dispositivo e l'autorizzazione dell'operazione contestata è conforme con la definizione di SCA.

Secondo i principi elaborati dal Collegio di Coordinamento, l'accertamento della conformità della procedura di autenticazione alla definizione di SCA contenuta nel d.lgs. n. 11/2010 non è di per sé dirimente per ritenere accertata la responsabilità del cliente, che sussiste, invece, nei casi di comportamento fraudolento del medesimo ovvero di suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Più di recente, il medesimo Collegio di Coordinamento ha chiarito che la previsione di cui all'art. 10, comma 2, d.lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente ad indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione, dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente.

Nel caso in esame, sulla base della documentazione versata in atti risulta che:

- l'accesso da parte del frodatore all'*home banking* della ricorrente ed il successivo *enrollment* del dispositivo dal quale è stata poi eseguita l'operazione contestata sono stati effettuati mediante inserimento di codici OTP inviati via sms "parlanti" al numero di cellulare della ricorrente, che la mettevano in guardia dal comunicare i medesimi codici a terzi;
- a fronte di quanto dichiarato nella denuncia, cioè che la prima telefonata al frodatore sarebbe stata effettuata ad un numero di cellulare, la ricorrente ha depositato uno *screenshot* dal quale risulta tale numero apparentemente non riconducibile all'intermediario;
- l'intermediario ha avvertito tempestivamente (prima dell'esecuzione dell'operazione contestata), tramite e-mail, la ricorrente dell'avvenuto *enrollment* di un nuovo dispositivo.

Sulla base delle circostanze sopra illustrate, il Collegio ritiene che l'intermediario abbia fornito elementi sufficienti a comprovare la sussistenza di una condotta gravemente colpevole della ricorrente, avendo dimostrato che, nella causazione del danno, è necessariamente intervenuto un fattore (comunicazione da parte della ricorrente ai malfattori dei codici OTP necessari per l'*enrollment* del nuovo dispositivo, dal quale è stata poi eseguita l'operazione contestata) sufficiente ad escludere la propria totale responsabilità ai sensi della normativa vigente. La mancanza di prova, da parte della ricorrente, in ordine alla circostanza che il numero di telefono al quale ha effettuato la prima telefonata risulti riconducibile all'intermediario, induce il Collegio a ritenere che, nella fattispecie, si sia in presenza di un'ipotesi di c.d. *phishing* tradizionale.

In tali circostanze, l'assenza di cautela del cliente appare difficilmente scusabile, trattandosi di fenomeni diffusamente noti, che qualunque utente dotato di normale avvedutezza e prudenza deve essere in grado di individuare, non facendosi trarre in inganno. In forza di quanto sopra, alla luce delle caratteristiche tecniche di sicurezza adottate dall'intermediario, si deve dunque concludere che l'operazione fraudolenta è stata resa possibile da un comportamento gravemente colposo della cliente, che ha omesso di

adottare tutte le cautele necessarie a custodire i codici di accesso e/o i dispositivi connessi.
Quanto sopra premesso, il Collegio, ferma la prova della SCA e la sussistenza della colpa grave della ricorrente, deve valutare se, sulla base delle circostanze del caso concreto in esame, la responsabilità della medesima possa essere ripartita con quella dell'intermediario. È, al riguardo, rilevante quale indice che può parzialmente affievolire la pur sussistente colpa grave della ricorrente, la circostanza per cui quest'ultima abbia potuto riporre legittimo affidamento circa la genuinità della seconda telefonata ricevuta, in quanto proveniente da un numero riconducibile all'intermediario, nonché del messaggio civetta, che si era inserito nella chat dei messaggi riferibili all'intermediario.
Secondo l'orientamento dei Collegi, una responsabilità concorrente dell'intermediario può essere riscontrata in presenza di uno dei suddetti indici. Sulla base dei principi sopra richiamati, il Collegio ritiene che, nel caso oggetto del presente procedimento, si riscontri la ricorrenza di tali fattispecie.
Ad avviso del Collegio, pertanto, nell'esecuzione dell'operazione contestata ha avuto rilievo, dal punto di vista del nesso di causalità, anche una verosimile disfunzione organizzativa dell'intermediario.
Il Collegio ritiene, infine, che sia priva di fondamento la doglianza della ricorrente, secondo cui l'intermediario sarebbe inadempiente rispetto alla richiesta di procedere al blocco dell'operazione impartitagli. Nel caso di specie, peraltro, anche in base alla documentazione versata in atti dalla resistente, risulta che l'intermediario ha immediatamente inoltrato apposito sms attestante l'avvenuta operazione.
In conclusione, alla luce di quanto sopra osservato in ordine alla conformità della procedura di SCA, alla sussistenza di una condotta gravemente negligente della ricorrente ed al contributo causale che le inefficienze tecnico-organizzative dell'intermediario hanno avuto rispetto alla produzione del danno patito dalla ricorrente, il Collegio stima equo liquidare a favore di quest'ultima un risarcimento pari ad €. 225,00=.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 225,00.
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
EMANUELE CESARE LUCCHINI GUASTALLA