COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) CORRADI	Membro di designazione rappresentativa degli intermediari
(BO) D ATRI	Membro di designazione rappresentativa dei clienti

Relatore MARCO CORRADI

Seduta del 03/12/2024

FATTO

Parte ricorrente afferma:

- che il 18 settembre 2023 apriva presso l'intermediario resistente un conto corrente "*online*" su cui accreditava la somma di € 3.500,00.
- Che, il successivo giorno 23 settembre, apriva, presso il medesimo intermediario, un conto corrente "*deposito flessibile*" su cui trasferiva la somma di € 3.500,00 in precedenza accreditata sul conto corrente.
- Di aver ricevuto, alle ore 15:14 del giorno 26 settembre 2023, una telefonata proveniente da un numero mobile, nel corso della quale l'interlocutore, spacciatosi per un funzionario dell'intermediario resistente, lo avvisava che erano stati accertati problemi di "*riallineamento*" sui conti correnti e che a breve sarebbe stato ricontattato dal servizio clienti.
- Di essere stato da lì a poco contattato, e più precisamente alle ore 15:33, dal numero verde dell'intermediario ed il "falso" operatore, dimostrando diretta conoscenza della situazione patrimoniale e contrattuale, lo informava che il conto corrente "*deposito flessibile*" era stato annullato e che la somma versata era stata nuovamente accreditata sul conto corrente "*online*". Il che effettivamente avveniva, senza che,

peraltro, lui avesse rilasciato alcuna autorizzazione.

- Che, come anticipato dall'interlocutore, gli erano, quindi, stati trasmessi, al fine di ripristinare il conto corrente "*deposito flessibile*" tre messaggi "SMS" contenenti i codici OTP necessari per effettuare tre bonifici di € 1.000,00 ciascuno che, secondo quanto affermato dal "falso" operatore, sarebbero dovuti servire a ripristinare la provvista sul conto corrente medesimo.
- Che gli era poi stato trasmesso un quarto messaggio "SMS" con OTP per un ulteriore bonifico di € 1.000,00 che non andava a buon fine per insufficienza dei fondi.
- Che per questa ragione era stato invitato a trasferire l'ulteriore somma di € 3.000,00 da un altro conto corrente intrattenuto presso un diverso intermediario dal cui servizio clienti, gli veniva anticipato, sarebbe pervenuta una telefonata di conferma.
- Di aver ricevuto, alle ore 15:43 dello stesso giorno, una telefonata dal numero verde ufficiale del diverso intermediario, nel corso della quale, in ragione della somiglianza di voce dell'interlocutore rispetto al precedente, si insospettiva e, conseguentemente, minacciava di sporgere querela. A quel punto, la telefonata era interrotta improvvisamente.
- Di aver, quindi, chiamato, alle ore 16:43, il numero verde della banca resistente e bloccato i conti a lui intestati tramite l'inserimento del codice OTP, pervenuto anch'esso, al pari di quelli relativi alle precedenti operazioni "*fraudolente*", tramite messaggio "SMS" proveniente dal medesimo contatto ufficiale.
- Che l'intermediario resistente, dopo aver riferito di non aver potuto ottenere dalla banca beneficiaria lo storno dei tre bonifici disconosciuti, rigettava la richiesta di rimborso perché, pur avendo dato atto che l'accesso all'area riservata mediante inserimento di "*password*" era avvenuta da un differente indirizzo IP, assumeva di aver inviato un "*messaggio push e una e-mail alla casella postale comunicata dal cliente"*.
- Che non è ravvisabile in suo capo alcun profilo di colpa grave vuoi per le modalità di svolgimento della truffa, connotata da un rapido concatenarsi dei fatti in uno strettissimo periodo temporale, vuoi per non aver egli mai comunicato al "falso" operatore le proprie credenziali statiche (*username* e *password*) necessarie per l'accesso e l'operatività del conto corrente "*online*" e del conto corrente "deposito flessibile" e per il perfezionamento delle operazioni disconosciute.
- Che il "falso" operatore non aveva inizialmente destato alcun sospetto, avendo dato prova di essere perfettamente a conoscenza dell'esistenza dei conti correnti aperti solo qualche giorno prima.
- Che la truffa si era perfezionata a causa dell'annullamento del conto corrente "deposito flessibile" disposto dall'autore dell'illecito che, peraltro, aveva acceduto all'*account* da un dispositivo diverso da quello certificato usualmente da lui utilizzato,
- Che l'avviso di tale sospetta operazione era pervenuto tramite mail alle ore 15:21, quando la truffa era già in fase di esecuzione e lui, essendo in quel momento a colloquio con l'autore dell'illecito, non aveva potuto averne effettiva conoscenza.
- Che appare configurabile, pertanto, una responsabilità dell'intermediario resistente per non avere esercitato il dovuto controllo sui propri sistemi al fine di evitare l'acquisizione da parte di terzi di informazioni riservate, nonché per non aver impedito l'accesso al conto corrente da un diverso IP e aver consentito l'annullamento del conto corrente "deposito flessibile" senza l'autorizzazione del cliente.

Parte resistente, in sede di controdeduzioni, eccepisce che:

- L'operazione disconosciuta è stata correttamente autorizzata mediante l'utilizzo delle credenziali statiche e dinamiche in possesso del ricorrente con autenticazione forte a due fattori, è stata registrata e contabilizzata senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la sua esecuzione.
- Per l'accesso all'area riservata, ai sensi dell'art. 10 del Regolamento Delegato (UE) n. 2018/839, è richiesta l'autenticazione forte mediante OTP, trasmessa via messaggio "SMS" all'utenza mobile indicata dal cliente in fase di apertura del rapporto e validata dalla Banca, nei casi di *(a)* primo accesso e *(b)* qualora siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha avuto accesso al conto corrente mediante autenticazione forte.
- Ove non venga effettuata l'autenticazione forte, l'accesso del cliente è limitato alle seguenti informazioni: saldo del conto corrente; operazioni di pagamento eseguite negli ultimi 90 giorni.
- I bonifici disconosciuti dal ricorrente sono stati inseriti all'interno dell'area riservata e confermati mediante OTP inviato all'utenza mobile del cliente.
- Il primo accesso all'area riservata del ricorrente da un indirizzo IP (93***183) diverso da quelli ordinariamente utilizzati è stato registrato alle ore 15:21:44 del 26 settembre 2023, mediante inserimento di "*username*" e "*password*" scelti dal ricorrente in fase di apertura del conto corrente.
- L'ultimo accesso all'area riservata del ricorrente mediante autenticazione forte registrato prima della frode è avvenuto in data 13 settembre 2023 alle ore 23:42:41.
- Aveva inviato al ricorrente una segnalazione via *push* nell'*app* e via mail dell'accesso all'area riservata del ricorrente mediante nuovo dispositivo, nonché le segnalazioni dell'addebito degli ordini di bonifico oggetto di frode.
- Il ricorrente ha violato con colpa grave l'art. 7 del D.lgs. 11/2010, condividendo numerosi codici con terzi "*malfattori*".

Parte ricorrente in sede di repliche deduce che:

- Dall'esame della documentazione prodotta dalla Banca è emerso che alle ore 15:21 del 26 settembre 2023 era stato effettuato un accesso all'area riservata da un indirizzo IP diverso rispetto a quelli comunemente da lui utilizzati, a seguito del quale era stato effettuato il cambio del dispositivo certificato: da quello effettivo, Android Xiaomi ad uno differente, Apple IPhone (evidentemente nella disponibilità del truffatore).
- Un'operazione così delicata, come il cambio del dispositivo certificato richiede maggiori controlli e tutele, in quanto la mail, peraltro generica, non può essere considerata idonea e sufficiente ad allertare ed informare adeguatamente il cliente.
- Il numero di codice OTP utilizzato per l'annullamento del "deposito flessibile" non era mai pervenuto sul suo dispositivo.

Parte resistente in sede di controrepliche eccepisce che:

- Diversamente da quanto affermato dal ricorrente, la Banca non esegue una certificazione del dispositivo utilizzato per accedere all'area personale del cliente, bensì in fase di apertura del rapporto contrattuale valida l'utenza mobile indicata dal cliente e univocamente associata al conto corrente.

- È, pertanto, il numero di telefono ad essere univocamente associato al conto corrente, ed è il cambio del numero di telefono ad essere soggetto sempre a una procedura rafforzata.
- I messaggi "SMS" contenenti le OTP necessarie ad autorizzare le operazioni di pagamento oggetto di frode, anche a fronte dell'accesso all'area riservata del ricorrente mediante un dispositivo differente, erano stati inviati unicamente all'utenza mobile indicata dal ricorrente in fase di apertura del rapporto contrattuale.

DIRITTO

Come già riferito in punto di fatto, il presente procedimento ha ad oggetto il disconoscimento di 3 bonifici di € 1,000,00 ciascuno, la cui provvista è stata creata mediante lo svincolo di un conto deposito flessibile.

Le operazioni contestate sono state poste in essere sotto il vigore del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Al riguardo, è opportuno, poi, ricordare che, ai sensi del primo comma dell'articolo 10 del citato D.lgs. 11/2010, è onere dell'intermediario provare che l'operazione sia 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, pena, in difetto, sopportare integralmente le conseguenze delle operazioni disconosciute.

Sul punto, l'intermediario resistente ha prodotto dei log da cui è possibile desumere che il primo accesso nell'area riservata del ricorrente da un indirizzo (IP 93.150.200.183 – Paese IP Avellino) diverso da quello ordinariamente utilizzato (IP 5.168.180.102 – Paese IP Bolonia) è stato registrato alle ore 15:21:44 del 26 settembre 2023; cioè sette minuti dopo l'inizio della prima conversazione intercorsa tra il ricorrente ed il falso operatore bancario e appena due minuti prima dell'operazione di "riaccredito" della somma di € 3.000,00 dal conto deposito flessibile al conto corrente *online*.

Accesso che è avvenuto con inserimento di username e password personali senza che sia stato richiesto l'inserimento anche di una OTP quale doppio fattore di autenticazione.

A tale proposito, l'intermediario ha tenuto a precisare che il ricorrente aveva eseguito l'accesso all'area riservata mediante *strong customer authentication* meno di 90 giorni prima di tale accesso, in data 13 settembre 2023 alle ore 23:42:41 e, pertanto, l'obbligo di SCA era di già stato assolto, giusta previsione di cui all'art. 10 del Regolamento Delegato (UE) 2018/839.

In merito, poi, al cambio di dispositivo, l'intermediario ha riferito di non certificare il dispositivo utilizzato dal cliente per accedere alla sua area personale, ma di validare esclusivamente, in fase di apertura del rapporto contrattuale, l'utenza mobile indicata dal cliente e univocamente associata al conto corrente.

La ricostruzione dei fatti fin qui resa impone al Collegio di attenzionare, prima di ogni altra, la circostanza che l'accesso nell'area personale del ricorrente da un diverso dispositivo è avvenuta senza il doppio fattore di autenticazione.

Orbene, è costante orientamento dei Collegi ABF quello di ritenere un accesso all'*home banking* eseguito tramite l'inserimento dei soli username e password non conforme alle prescrizioni normative in materia di SCA, atteso che mentre la password costituisce un elemento di conoscenza, lo username non rappresenta invece un fattore idoneo ai fini SCA.

Da tale orientamento, che il Collegio condivide pienamente, non ci si può discostare per via del fatto che nel caso concreto vi è stato un accesso mediante SCA nei 90 giorni precedenti al 26 settembre. Sul punto, difatti, l'EBA ha chiarito che, nei casi di esenzione dalla SCA di cui all'art. 10 del regolamento delegato UE 2018/389 e qualora l'intermediario decida di non adottare l'autenticazione forte, resta ferma la responsabilità di quest'ultimo (fatta salva la frode dell'utilizzatore) tutte le volte che le operazioni siano state disconosciute dal cliente (cfr. EBA Q&A 2018-4042).

Ora non può tacersi la circostanza che, nella fattispecie, il primo accesso dal diverso dispositivo ha avuto quale finalità quella del trasferimento delle somme dal conto di deposito flessibile al conto corrente *on line*, così da risultare costituita la provvista necessaria per poi eseguire le tre operazioni di bonifico che hanno determinato l'effettiva perdita patrimoniale in capo al ricorrente. Sicché, diviene fondamentale accertare se l'operazione di acquisizione della provvista possa o meno considerarsi, nel caso di specie, fonte diretta del pregiudizio economico patito dal ricorrente.

In tema è di recente intervenuto il Collegio di Coordinamento che, con decisione n. 8671/2024, ha avuto modo di enunciare il seguente principio di diritto: "*I pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario possono essere sottratti all'obbligo della SCA anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente*".

Va detto, però, che nel caso esaminato dal Collegio di Coordinamento la perdita patrimoniale subita dal ricorrente non era stata ritenuta conseguenza immediata e diretta di un inadempimento dell'intermediario, in quanto derivante dal compimento da parte del cliente medesimo di pagamenti verso terzi. In altri termini, la condotta del cliente era stata capace di interrompere il nesso causale fra l'assenza della SCA ed il pregiudizio finale da questi subito.

Caso che diverge in maniera netta dalla fattispecie concreta, laddove è stato il truffatore ad eseguire l'accesso (login), quindi il trasferimento dei fondi da un conto all'altro, quindi le operazioni di bonifico costituenti la perdita patrimoniale subita dall'attuale ricorrente. Il quale ultimo non ha tenuto alcuna condotta fattiva ed omissiva che sia stata idonea a interrompere il nesso causale di cui sopra si è detto. A nulla valendo, in senso contrario, il fatto che l'intermediario, in fase di esecuzione del trasferimento dell'importo di € 3.000,00 dal conto deposito flessibile al conto corrente *on line* abbia inviato un messaggio contenente l'OTP all'utenza mobile del ricorrente, poiché il contenuto dello stesso non esplicita il tipo di operazione per cui era trasmessa la password temporanea, limitandosi ad affermare: "*Per eseguire la tua operazione*".

Alla luce di quanto risultante in punto di fatto e di diritto, il Collegio ha raggiunto il convincimento che, nel caso in esame, l'intermediario non ha adempiuto all'onere su di esso gravante di corretta e completa prova della SCA nella fase di login, ritenuta

indispensabile per l'esecuzione delle successive operazioni che senza soluzione di continuità hanno determinato la perdita patrimoniale in capo al ricorrente.

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 3.000,00 (tremila/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