COLLEGIO DI ROMA

composto dai signori:

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

Relatore NOAH VARDI

Seduta del 20/03/2023

FATTO

1. Parte ricorrente si rivolge all'Arbitro chiedendo la restituzione della somma di € 92.196,21, corrispondente a n. 43 bonifici istantanei effettuati il 28/02/2022 a valere sul proprio conto corrente aziendale, all'esito di una truffa. Chiede altresì, il risarcimento del danno.
2. Il ricorrente è titolare di un conto corrente aziendale detenuto presso l'intermediario resistente. Riferisce che la sera del 28/02/2022 è rimasto vittima di una frode nel corso della quale il truffatore lo ha contattato telefonicamente tramite un numero di telefono riconducibile all'intermediario, fingendosi un operatore. In particolare, l'interlocutore ha prospettato la necessità di verificare l'operatività del conto, rispetto al quale sarebbe altrimenti cessata la possibilità di accedere online. Confidando nella genuinità di tali affermazioni, sulla base di un affidamento ingenerato dal numero del chiamante, il ricorrente ha generato i codici richiesti tramite il proprio *token*. A questo punto, il frodatore ha affermato che fosse stato raggiunto il tempo massimo di conversazione telefonica. Ha quindi interrotto la telefonata ed ha ricontattato il ricorrente tramite un diverso numero telefonico. La conversazione si è protratta per circa un'ora. Terminata la chiamata, il ricorrente è stato raggiunto da un'ulteriore telefonata, da parte di un sedicente funzionario della polizia postale. L'interlocutore affermava che egli fosse stato vittima di una frode informatica, destando i sospetti del ricorrente, che si è infine

avveduto che si trattava di una frode. Alle 00:26 del 01/03/2022 il ricorrente ha inviato un'e-mail all'indirizzo dell'intermediario. Nel pomeriggio ha ricevuto riscontro, in cui lo si invitava a contattare telefonicamente l'assistenza clienti. La mattina del 01/03/2022 il ricorrente si è recato presso lo sportello della propria banca, constatando l'effettiva entità della truffa, concretizzatasi in un esborso complessivo di 92.196,21 €, tramite n. 43 bonifici istantanei. Riferisce che peraltro, il conto corrente aziendale del ricorrente non è autorizzato all'esecuzione di bonifici istantanei.

Tanto premesso in fatto, il ricorrente osserva che la banca convenuta aveva il dovere di adottare tutte le misure idonee a garantire la sicurezza del servizio, con la diligenza richiesta *ex* art. 1176 c. 2 c.c., che, come rammentato dalla Suprema Corte di Cassazione, ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento e assumendo come parametro la figura dell'accorto banchiere (Cass. civ., Sez. I, 19/01/2016, n. 806). Ciononostante, l'intermediario non ha impedito che terzi accedessero al conto corrente del ricorrente. Inoltre, la banca ha mancato di bloccare cautelativamente il conto del ricorrente a fronte della movimentazione sospetta. Infatti, ogni intermediario finanziario è tenuto ad eseguire una obbligatoria profilatura del cliente onde accertare se una determinata operazione risulta coerente con il profilo composto dai dati raccolti e con l'operatività storica documentata dai movimenti eseguiti dal cliente. Ciò posto, il ricorrente domanda il rimborso delle somme indebitamente sottratte, oltre al risarcimento del danno da quantificare in 4.000,00 € e alle spese legali.

3. In sede di controdeduzioni, l'intermediario riferisce che il ricorso ha ad oggetto bonifici istantanei disposti il 28/02/2022, a valere sul conto corrente del ricorrente. Il conto corrente in questione è un conto destinato alle imprese, che consente di nominare un "supervisore" abilitato ad operare sullo stesso, al quale vengono consegnate le credenziali e il *token* fisico da utilizzare per operare online. Quanto all'autenticazione, sia l'accesso all'*home banking* sia ciascuna operazione dispositiva è stata autorizzata tramite un doppio fattore di autenticazione: le credenziali statiche fornite in sede di apertura del conto (una password per accedere all'*home banking* e un PIN per autenticare le singole operazioni); un codice OTP generato tramite *token* fisico, anch'esso consegnato al momento della sottoscrizione. Quanto alla colpa grave, deduce che il mero impiego di un'autenticazione forte può far presumere la negligenza dell'utilizzatore, secondo l'orientamento dell'ABF. Peraltro, le dichiarazioni rilasciate dal ricorrente in sede di denuncia inducono a rinvenire una sua colpa grave. Infatti, egli ha dichiarato di aver seguito le istruzioni telefoniche del sedicente frodatore, comunicando tutti i codici OTP generati dal *token* in suo possesso. Il ricorrente avrebbe dovuto insospettirsi tenendo conto dell'orario in cui si è svolta la telefonata, della sua durata e del fatto che la seconda parte della conversazione si è svolta tramite un numero non riconducibile all'intermediario. Inoltre, non avrebbe comunque dovuto riporre troppa fiducia nel *caller ID* indicato dalla prima telefonata, riconducibile alla banca resistente. Infatti, esso può essere notoriamente emulato e non garantisce la provenienza della telefonata, com'è avvenuto anche nel caso di specie, dato che non è stato rinvenuto alcun malfunzionamento nelle reti dell'intermediario. A seguito della presentazione del reclamo, l'intermediario non ha ripristinato il saldo del conto corrente a fronte di un motivato sospetto di frode, *ex* art. 11, comma 2 del d.l. 11/2010. Nel ricorso si afferma che sul conto aziendale non fosse autorizzata l'esecuzione di bonifici istantanei. Ciò non corrisponde però al vero, dato che tale facoltà era prevista sin dalla sottoscrizione del contratto, come risulta dal documento di sintesi. Quanto alla richiesta di risarcimento del danno patrimoniale e non patrimoniale, essa è completamente

sprovvista di prova circa l'*an*, il *quantum* e il nesso di causalità. L'intermediario chiede pertanto il respingimento del ricorso in ogni sua parte in quanto infondato nel merito.

4. In sede di repliche, oltre a ribadire quanto già allegato, parte ricorrente sostiene che nelle controdeduzioni l'intermediario afferma che il soggetto "supervisore" del conto sia il ricorrente, ma indica un codice fiscale errato. Sostiene che l'intermediario non ha dimostrato la colpa grave del ricorrente, il quale confidava legittimamente nella genuinità della conversazione telefonica in quanto effettuata tramite il numero dell'intermediario, il cui utilizzo improprio è a quest'ultimo imputabile. Ha generato e comunicato i codici OTP solo perché riteneva di favorire, così facendo, il ripristino della regolare funzionalità del conto. Afferma che in base al documento di sintesi del c/c prodotto dall'intermediario con le controdeduzioni, il servizio di bonifico in tempo reale prevede un orario limite di ricezione per le 17:00, mentre le operazioni in questione sono state eseguite tra le 21:15 e le 22:21. Quindi l'istituto non avrebbe dovuto autorizzare l'effettuazione di simili operazioni, intervenute oltre l'orario limite previsto dal contratto. Diversamente da quanto previsto dall'art. 11, comma 1, d.l. n. 11/2010, l'intermediario non ha immediatamente riaccreditato le somme sottratte sul conto del ricorrente a seguito del reclamo. Afferma di aver mancato tale adempimento in forza di un sospetto di frode *ex* art. 11, comma 2, d.l. cit. Tuttavia, in queste ipotesi si prevede un'immediata comunicazione scritta alla Banca d'Italia di cui l'intermediario resistente non ha dato prova. Inoltre, l'intermediario non ha attivato il servizio di SMS *alert*, che avrebbe invece dovuto essere attivato in via automatica, a prescindere da un'esplicita richiesta del cliente, secondo l'orientamento consolidato dell'ABF (cfr. Collegio di Coordinamento, decisione 06/11/2019, n. 24366).
5. In sede di controrepliche, oltre a ribadire quanto già allegato, parte resistente osserva che come rilevato dal ricorrente, nelle controdeduzioni è stato riportato un codice fiscale errato in corrispondenza del soggetto "supervisore" del conto. Si tratta di un mero refuso e il codice fiscale corretto è quello del ricorrente, che emerge anche dai log in atti. Nel caso in esame, l'unico artefice del danno è stato il ricorrente, il quale ammette di aver seguito le indicazioni del frodatore e le credenziali di accesso all'*home banking* al presunto frodatore, incluse tutte le numerose OTP – una per la login ed una per ciascuna operazione dispositiva – generate dal *Token* Fisico in suo possesso. Ciò integra un comportamento gravemente colposo. Ciò nonostante numerose circostanze avrebbero dovuto insospettirlo, tra cui: l'ora tarda, la durata della telefonata e il fatto che fosse poi stato ricontattato tramite un numero non riconducibile all'intermediario.

DIRITTO

1. Il ricorso ha ad oggetto il disconoscimento di n. 43 operazioni di bonifico istantaneo pari alla somma complessiva di euro 92.196,21 eseguite in data 28/02/2022 all'esito di una truffa. Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). Alle stesse sono inoltre applicabili le disposizioni del Regolamento delegato (UE) della Commissione 2018/389, che stabilisce i requisiti dell'autenticazione forte ai sensi della PSD 2. Vengono in rilievo le norme contenute nell'articolo 10, comma 1 e comma 2, e nell'articolo 12, comma 3, del d.lgs. n/2010. Ove il pagatore abbia dimostrato, anche solo in via presuntiva, che lo strumento di pagamento è stato oggetto di utilizzo non autorizzato, graverà sul prestatore di servizi di pagamento l'onere probatorio previsto dall'articolo 10, comma 2, d.lgs. n.11/2010 con riguardo alla frode, dolo o colpa grave del pagatore,

al fine di stabilirne il grado di responsabilità ai sensi dell'art.12 d.lgs. 11/2010. Parte ricorrente allega di aver subito una truffa, come attestato dalla denuncia agli atti e dalle circostanze riferite nel ricorso, apparentemente perpetrata con la tecnica di *vishing* con *caller ID spoofing.*

Dalla denuncia in atti risulta infatti quanto segue: il ricorrente riferisce che alle 21:00 del 28/02/2022 è stato raggiunto da una telefonata che riportava il *caller* ID dell'intermediario e – a fronte delle prospettazioni di un sedicente operatore circa il potenziale blocco del servizio – egli ha comunicato i codici dinamici OTP richiesti dal frodatore, generati tramite un *token* fisico in suo possesso. Sempre in base alla denuncia, ad un certo punto della telefonata l'operatore si è congedato momentaneamente, per poi richiamare il ricorrente da un numero di cellulare non riconducibile all'intermediario, e guidarlo in ulteriori attività. All'esito delle operazioni, il truffatore ha raccomandato al ricorrente di non effettuare accessi al suo *home banking* per almeno 24 ore. Poco dopo, il ricorrente è stato contattato, tramite un numero cellulare, da un altro soggetto, che si spacciava per un vice ispettore della polizia Postale e gli chiedeva di riferire le proprie credenziali per metterlo al riparo da una frode in corso. La telefonata di questo secondo interlocutore ha portato il ricorrente a insospettirsi e porre domande al frodatore, il quale ha interrotto la conversazione. Il giorno successivo, il ricorrente ha verificato la consistenza del proprio conto aziendale recandosi presso la sede dell'intermediario e ha rilevato la sottrazione di 92.196,21 € tramite numerosi bonifici.

La fattispecie impone che venga valutata innanzitutto l'adeguatezza del sistema di protezione adottato dell'intermediario nell'autorizzazione delle operazioni di pagamento. Dalle allegazioni dalle parti e dagli atti prodotti dall'intermediario (log delle transazioni) risulta che le operazioni contestate sono state autenticate tramite un elemento di conoscenza- le credenziali statiche di accesso per l'*home banking* e la digitazione del PIN per ogni operazioni- e un elemento di possesso costituito da OTP generati da un *token* fisico a disposizione del ricorrente. Tale sistema è considerato dall'EBA conforme alla *strong customer authentication*.

Il ricorrente conferma di aver comunicato al frodatore i codici OTP generati dal proprio *token* fisico, durante telefonata fraudolenta. Infatti, le modalità della frode, come quella in esame, sono riconducibili alle ipotesi di *vishing* con *ID caller spoofing*, in cui la chiamata truffaldina proviene apparentemente da un numero riconducibile all'intermediario: il ricorrente, fidandosi della genuinità della chiamata ricevuta ha autorizzato le operazioni. Sul punto, il Collegio, come già in passato, osserva che con riferimento alla condotta del ricorrente, non assume rilevanza il fatto che le chiamate ricevute apparissero provenire dal numero verde del servizio clienti dell'intermediario: infatti il carattere anomalo delle richieste rivolte al ricorrente, l'ora della telefonata e le altre circostanze quali le successive chiamate da utenze mobili, avrebbero dovuto indurre il ricorrente a prestare maggiore attenzione e a non seguire pedissequamente le istruzioni del falso operatore. (Cfr. Collegio Roma, dec. n. 16489/2021; dec. n.1209/2021; dec. n. 17334/2021). La condotta del ricorrente è stata quindi negligente e sussistono profili di colpa grave.

Il Collegio ritiene tuttavia che l'efficienza causale di tali profili non sia stata esclusiva nel produrre il danno. Il Collegio osserva infatti, che le modalità di svolgimento della truffa richiedano di considerare anche l'obbligo di monitoraggio delle operazioni di pagamento da parte dell'intermediario. Il numero elevatissimo di operazioni (43 bonifici istantanei in uscita, oltre a 5 bonifici istantanei in entrata recanti la dicitura "per payment return" (verosimilmente in quanto respinti dalla

banca del beneficiario) eseguite in un lasso di tempo ridottissimo (poco più di un'ora e mezza, tra le 21.15 e le 22.53 del 28/02/2022)) è idoneo a ritenere sussistente un rischio di frode. L'art. 8, d.m. 30 aprile 2007, n. 112 sull'istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento, indica infatti che "Si configura il rischio di frode di cui all'articolo 3, comma 1 della legge, quando viene raggiunto uno dei seguenti parametri: (…) b) riguardo alle carte di pagamento sottoposte a monitoraggio di cui all'articolo 7, lettera c): 1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento". Di fronte a un rischio normativamente tipizzato, sebbene tale decreto si riferisca alle operazioni con carta, questo Arbitro ritiene che l'intermediario avrebbe dovuto attivarsi per evitare tale rischio (cfr. Collegio di Roma dec. n. 7426/2022 e dec. n. 17037/2020). D'altra parte, è lo stesso art. 2 del Regolamento Delegato (UE) n. 2018/389 della Commissione a prevedere che gli intermediari predispongano meccanismi di monitoraggio in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente. A fronte quindi di tali elementi indicativi di un rischio di frode, un'efficiente sistema di monitoraggio avrebbe dovuto bloccare le operazioni sospette.

Dalle allegazioni di parte e dalla documentazione in atti inoltre, non risulta nemmeno l'attivazione del sistema di *sms alert*; la mancanza di attivazione di tale sistema viene ritenuta da codesto Collegio una disfunzione organizzativa, che come stabilito dal Collegio di Coordinamento ABF (dec. n. 16237/2018) è "di per sé idonea a spostare verso l'intermediario il rischio connesso ad operazioni fraudolente avvenute con l'impiego di tali strumenti (…), configurando un'ipotesi di responsabilità da inadeguata organizzazione imputabile esclusivamente all'intermediario resistente".

Pertanto, il Collegio ritiene che anche la condotta dell'intermediario sia caratterizzata da profili di colpa ed abbia contribuito causalmente alla produzione del danno ai sensi dell'art. 1227, 1°comma, c.c.; accoglie quindi parzialmente il ricorso e per l'effetto dispone che le conseguenze dannose derivanti dalle disposizioni indebite siano poste a carico delle parti in proporzione delle rispettive responsabilità.

Quanto alla richiesta di risarcimento del danno avanzata dal ricorrente e quantificata in €.4.000,00, il Collegio osserva che in merito, non essendo stato allegato né documentato alcunché, non è stato assolto l'onere probatorio gravante sul ricorrente. Lo stesso dicasi per la domanda di rimborso delle spese legali. Le domande di risarcimento e di rimborso delle spese legali non vengono pertanto accolte.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 45.000,00, 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