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) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore ANDREA GENOVESE

Seduta del 05/07/2023

FATTO

Con ricorso n. 0058645 dell'11.1.2023, la parte ricorrente, rimasta insoddisfatta dell'interlocuzione intercorsa con l'intermediario nella fase del reclamo, si rivolge all'Arbitro al quale chiede la sua condanna alla restituzione della somma complessiva di € 18.000,00, oltre interessi, corrispondente all'importo di sei operazioni di pagamento eseguite da terzi non autorizzati e disconosciute. Il tutto con il favore delle spese di assistenza difensiva quantificate in € 300,00. A sostegno della pretesa, deduce in particolare: i) di essere intestataria del conto corrente nr. ***765, intrattenuto con l'intermediario, gestito anche dalla moglie T.M.A.; ii) in data 20.4.2022, alle ore 14:48, quest'ultima riceveva sul proprio telefonino un sms apparentemente proveniente dall'intermediario, con il quale veniva invitata a cliccare su di un link. Contestualmente, il gestore telefonico le comunicava il mancato rinnovo della promozione che sarebbe dovuta avvenire mediante addebito sul conto; iii) di avere cliccato sul link presente nel messaggio civetta dal quale si accedeva ad una pagina web contenente il logo della banca, dove le veniva chiesto di inserire il codice cliente, il pin e il numero di cellulare per la verifica di sicurezza web relativamente alle carte di debito; iv) di avere ricevuto alle ore 15:18 sulla medesima utenza mobile un secondo messaggio sms, anch'esso apparentemente proveniente dalla banca, con il quale veniva invitata a rispondere ad una successiva telefonata che avrebbe ricevuto da parte di un operatore telefonico. Riceveva la preannunciata telefonata da parte di chiamante con numero identico a quello riconducibile all'intermediario, in occasione della quale le venivano riferite alcune criticità quanto alla

sicurezza dell'applicazione di *home banking* in uso. Giacché non titolare del conto, la sig.ra T.M.A. chiedeva all'ignoto operatore di richiamarla più tardi, verso ore 16:30/17:00, quando sarebbe stato presente in casa il marito, intestatario del conto; v) alle ore 16:36, veniva nuovamente contattata sul telefono fisso dal sedicente operatore il quale le riferiva che, per poter ripristinare la sicurezza del sistema, era necessario disinstallare l'app della banca e installare una nuova applicazione denominata "banca sicura". A tal fine, venivano comunicati alla parte ricorrente con sms e due email alcuni codici numerici. Il sedicente operatore rappresentava alla parte ricorrente che avrebbe ricevuto un ulteriore sms che le avrebbe consentito di reinstallare l'applicazione di *home banking* e di utilizzare i servizi *online*, fissando al contempo un nuovo appuntamento telefonico per il giorno seguente; vi) non avendo ricevuto altre notizie dal fantomatico operatore, il giorno successivo verso le ore 17:15 contattava il numero verde della banca, per poi recarsi all'indomani presso un ATM allorché poteva constatare che terzi ignoti avevano eseguito sei bonifici da € 3.000,00 ciascuno, per una somma complessiva di € 18.000,00; vii) di avere sporto la denuncia e presentato reclamo nei confronti dell'intermediario, riscontrato negativamente; viii) di avere subito una truffa sofisticata in considerazione del fatto che i messaggi civetta si inserivano nello storico delle comunicazioni intrattenute con la banca. Le telefonate del sedicente operatore sembravano inoltre provenire dal numero verde della stessa banca; ix) di avere diritto al rimborso dell'importo € 18.000,00, oltre agli interessi maturati, nonché delle spese legali quantificate in € 300,00.

Costituitosi, l'intermediario si oppone alle avverse pretese, in particolare deducendo che: 1) i sei bonifici del 20.4.2022 disconosciuti dalla parte ricorrente sono stati inseriti ed autorizzati *online* attraverso l'uso delle credenziali di sicurezza in dotazione a quest'ultimo; 2) il ricorrente ha rilasciato la procura alla moglie T.M.A. autorizzandola ad operare sul proprio conto corrente; 3) la parte ricorrente ha aderito al servizio SMS Alert, collegato al proprio telefono cellulare n. 333***258, corrispondente a quello indicato nella querela; 4) l'accesso alle funzioni di *inquiry* e dispositive avviene tramite un sistema con autenticazione forte. In particolare, per l'accesso alla *home banking* da App è necessario l'inserimento del numero cliente, del PIN e del codice OTP, codice dinamico generato da *Mobile* Token; per disporre le operazioni è invece indispensabile l'inserimento del PIN e della OTP. Precisa, inoltre, che al cliente è consentito attivare il *Mobile Token* su due dispositivi contemporaneamente e che, inoltre, lo stesso è libero di sostituire il proprio *device* senza dover comunicare il nuovo modello alla banca, laddove il numero di cellulare resti invariato. Rappresenta anche che l'attivazione del *Mobile Token* è possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente in parte via *mail* e in parte via sms al cellulare certificato; 5) nel caso in esame, in data 20.4.2022, rispettivamente alle 17:02 e alle 17:04, la banca ha inviato una *mail* alla casella di posta del cliente e un sms cellulare certificato con il codice OTP necessario per attivare il *Mobile Token*, avente il seguente contenuto: "Stai attivando il Mobile Token. Ricordati che il personale *** non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: ***". Sulla base di ciò, parte resistente ritiene di avere adottato un sistema di autenticazione forte; 6) dalle deduzioni di controparte si evince che il raggiro è stato operato nei confronti della sig.ra T.M.A., destinataria del primo sms civetta, la quale non era la titolare del conto corrente, né titolare del servizio di *home banking*, con la conseguenza che sul suo cellulare non avrebbe potuto attivare alcuna App. L'intermediario ritiene, quindi, che durante la telefonata delle ore 17:00, quando è stato chiesto dai malfattori di disinstallare l'app della banca, i clienti avrebbero dovuto insospettirsi e interrompere la telefonata, non sussistendo alcuna motivazione per sostituire l'App ufficiale con una applicazione avente denominazione non riconducibile all'intermediario; 7) la truffa si è realizzata anche a causa dell'utilizzo

improprio delle credenziali da parte della moglie del ricorrente; credenziali che sono state comunicate a terzi, anche mediante inserimento delle stesse su sito non appartenente alla banca. Con riguardo agli sms illeciti, rappresenta che i *link* ivi indicati non risultano riconducili a quest'ultima. In merito al canale di provenienza degli SMS e delle telefonate, richiama l'attenzione sul fatto che il "caller ID" che appare su telefono fisso o mobile non garantisce l'autenticità della chiamata; 8) parte ricorrente è stata vittima di una frode di tipo classico resa possibile grazie alla colpa grave nella quale è incorsa, per avere omesso di adempiere, con la dovuta diligenza, ai propri obblighi di custodia e di protezione delle credenziali di sicurezza personali. Rappresenta inoltre che dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi, risultando per converso le operazioni correttamente autenticate, registrate e contabilizzate, come provato dai log prodotti in atti. In particolare, rappresenta che dalle evidenze informatiche risulta: a) un *login* alle 16:56 del 20.4.2022 con inserimento del PIN e dell'OTP, generato da *Mobile Token* con il *device* LG K10 2017 (LG-M250), con il quale è poi stato rimosso alle ore 16:58 del medesimo giorno il *Mobile Token*; b) un tentativo di accesso (propedeutico alla installazione del *Mobile Token*) il 20.4.2022 alle 17:01 mediante inserimento del PIN da un diverso *device* (realme C25Y), dove è stato poi attivato il *Mobile Token* alle 17:05 mediante inserimento del PIN e dell'OTP ricevuto via sms; c) un *login* alle 17:05 con verifica a 2 fattori mediante l'inserimento dell'OTP generato dal *Mobile Token* e l'inserimento di un bonifico alle 17:08 per l'importo di € 2.999,00 (oltre € 1,00 di commissione), autorizzato con PIN e OTP; d) l'inserimento di altri cinque bonifici in data 20.4.2022, rispettivamente alle ore 17:08, 17:09, 17:09, 17:09, 17:10, per l'importo di € 2.999,00 (oltre 1,00 euro di commissione) ciascuno; 9) dopo il disconoscimento delle operazioni, la banca ha tentato di recuperare i bonifici con la procedura di *recall* conclusi tuttavia con esito negativo; 10) la domanda di rimborso formulata dalla parte ricorrente deve, pertanto, ritenersi infondata, ragion per cui la banca chiede che il ricorso venga rigettato.

In sede di repliche, la parte ricorrente contesta delle avverse deduzioni, assumendo, in particolare, di non avere ricevuto alcun sms *alert* o notifica *push* in relazione alle operazioni di pagamento. Assume che dai log prodotti dall'intermediario gli avvisi risulterebbero inviati ad altro *device*. Contesta, inoltre, l'omessa rilevazione da parte dell'intermediario del carattere anomalo delle operazioni disconosciute. Nega di avere comunicando a terzi il codice PIN e OTP, precisando che per l'accesso all'*home banking* sarebbe richiesto solamente il fattore di conoscenza e non anche quello di possesso. Insiste per l'accoglimento del ricorso.

In sede di controrepliche, la parte resistente contesta le averse deduzioni, insistendo a sua volta per il rigetto del ricorso.

DIRITTO

La domanda di parte ricorrente è relativa all'accertamento del proprio diritto ad ottenere dall'intermediario convenuto la restituzione della somma di € 18.000,00, sottrattele fraudolentemente da terzi mediante sei operazioni di pagamento poi disconosciute, oltre a interessi e spese.

La materia è regolata dalle norme generali in tema di adempimento delle obbligazioni e di diligenza del mandatario (art. 1710 c.c.) e della banca nell'"Esecuzione d'incarichi" (art. 1856 c.c.), nonché dal D.lgs. 27.01.2010, n. 11, come modificato dal D.lgs. 15.12.2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13.01.2018. Le fonti normative che

regolano la *strong customer authentication* (c.d. SCA) sono rinvenibili negli artt. 97 e 98 della PSD 2, nell'articolo 10 *bis* del D.lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA, recepite con regolamento delegato UE n. 2018/389 della Commissione Europea, applicabile a far data dal 14.9.2019, nonché nei criteri interpretativi forniti dall'EBA, ad esempio attraverso il parere del 21.12.2019. In particolare, si osserva che il citato D.lgs. n. 10/2011 mentre, da un lato, impone agli intermediari, nella loro qualità di prestatori di servizi di pagamento, specifici obblighi di precauzione, primo fra tutti quello di garantire l'inaccessibilità dei dispositivi di pagamento a soggetti non autorizzati, dall'altro, istituisce il seguente regime di speciale protezione e di altrettanto speciale favore probatorio a beneficio degli utilizzatori: a) in caso di disconoscimento di un'operazione di pagamento, è onere dell'intermediario dimostrare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata e che la stessa non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; b) l'apparente corretta autenticazione non è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la disconosca; c) la responsabilità dell'utilizzatore resta dunque circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo inadempimento con dolo o colpa grave agli obblighi che l'art. 7 del decreto pone a suo carico, che si limitano nella richiesta di utilizzazione dello strumento di pagamento in conformità ai patti contenuti nell'accordo quadro che regola il servizio e alla tempestiva denuncia di furto, smarrimento, distruzione o altro uso non autorizzato dello strumento. Tutto ciò, con la precisazione che, ove una simile responsabilità non possa affermarsi in capo al cliente utilizzatore, quest'ultimo non sopporta le conseguenze dell'uso fraudolento o comunque non autorizzato del mezzo di pagamento se non nei limiti, eventualmente stabiliti nel contratto quadro, di una "franchigia" non superiore a € 50 (art. 12, commi 1° e 4°, D.lgs. 11/2010). Per quanto concerne l'onere della prova, si evidenzia che l'art. 10, comma 2° del D.lgs. n. 11/2010, 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". Sul punto, va richiamata la decisione n. 22745/2019 del Collegio di Coordinamento, con la quale è stato affermato "che la previsione normativa diretta a porre in modo esplicito l'onere della prova a carico del PSP è contenuta in un complesso di norme (quelle del decreto legislativo n. 218/2017) volte ad introdurre nella legge che regola la materia dei servizi di pagamento disposizioni rafforzative del «regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori», cui si fa riferimento nell'ordinanza con richiamo a varie pronunce del Collegio di coordinamento. E in effetti la nuova disposizione sull'onere probatorio di cui al comma 2 dell'art. 10 va a potenziare la tutela dell'utente il quale, nell'utilizzo degli strumenti di pagamento, può restare vittima di attività fraudolente che, allo stato delle conoscenze tecnologiche, possono prevalere sui presidi di sicurezza approntati dal PSP, senza che al comportamento dell'utilizzatore possa riconoscersi alcuna efficienza causale (o quanto meno non determinante) nella produzione del fatto illecito". In tal modo, il Collegio di Coordinamento ha posto in evidenza come non sia coerente con il dettato dell'art. 10 e le sottostanti scelte di politica legislativa la tendenza a procedere in via autonoma all'accertamento della colpa grave del ricorrente e a desumerne la sussistenza, in via presuntiva, dagli elementi conoscitivi acquisiti agli atti e in particolare dalle informazioni documentate fornite dal prestatore di servizi di pagamento al fine di provare l'"autenticazione" e la regolarità delle operazioni contestate. Pertanto, se l'intermediario attesta l'integrità ed il corretto funzionamento del proprio sistema informatico, ciò non equivale a provare che l'intrusione abusiva è imputabile al dolo o alla colpa grave dell'utente del servizio, perché l'esperienza dimostra l'ampia diffusione di frodi

informatiche talmente sofisticate da carpire la buona fede anche di quelle persone che sono solite agire in maniera avveduta e diligente.

Nel caso in esame, il Collegio osserva che i sei bonifici disconosciuti, di importo pari ad € 2.999,00 ciascuno, sono stati disposti in data 20.4.2022 tra le ore 17:08 e le ore 17:10.

Al riguardo, l'intermediario ha prodotto evidenze informatiche dalle quali emerge il sistema di autenticazione a due fattori utilizzato, sia per l'accesso all'*home banking* da App, sia per l'esecuzione delle operazioni dispositive. In particolare, parte resistente deduce che per effettuare il *login* e le operazioni di *inquiry* è necessario l'inserimento del numero cliente, del codice PIN e del codice OTP, codice dinamico generato da *Mobile Token*; per disporre le operazioni, le stesse devono essere inoltre confermate con l'inserimento del PIN e della OTP generata da *Mobile Token*.

Per quanto riguarda l'attivazione del *Mobile Token* è indispensabile la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via sms al cellulare certificato, come risulta dai *log* prodotti. Dall'esame di questi, in particolare, risulta che il 20.4.2022 alle 17:05 è stato attivato il *Mobile Token* mediante inserimento del PIN e di un codice OTP, che è stato inviato tramite sms al numero di cellulare certificato del ricorrente, corrispondente a quello indicato da quest'ultimo in sede di ricorso ABF.

Si pone in rilievo, inoltre, che il detto OTP risultante dai *log* è il medesimo che risulta indicato nel messaggio prodotto dal ricorrente (OTP "89724866"). Risulta provato, infine, che l'intermediario al fine della esecuzione delle operazioni di pagamento ha adottato un sistema di autenticazione basato sull'utilizzo del *Mobile Token* integrato nell'app, generatore di un codice OTP (fattore di possesso) e sull'inserimento di codice PIN (fattore conoscenza). Dalla documentazione prodotta, risulta anche l'invio degli sms *alert* sulla utenza telefonica certificata del ricorrente.

Secondo l'attuale stato della tecnica, questo sistema multifattoriale appare certamente idoneo a garantire un elevato livello di sicurezza, in conformità agli standard definiti dagli orientamenti dell'*European Banking Authority* del 21.6.2019 in materia di autenticazione forte. Si ritiene, dunque, che l'intermediario ha provato la corretta autenticazione, esecuzione e contabilizzazione delle operazioni contestate.

Per quanto concerne la condotta posta in essere dal ricorrente, il Collegio osserva che la schermata dei messaggi civetta sms ricevuti in data 20.4.2022 appaiono inviati dallo stesso contatto dell'intermediario, al pari della successiva telefonata intercorsa con il sedicente operatore. Tuttavia, negli stessi messaggi si rinvengono indici di inattendibilità e anomalia, in particolare il fatto che i *link* non sono riconducibili all'intermediario.

Secondo la più recente posizione condivisa dai Collegi territoriali, nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, a meno che non si rinvengano indici di inattendibilità o anomalia del messaggio, come accaduto nel caso di specie. In questi casi può quindi essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento delle operazioni orchestrate dal terzo non autorizzato, similmente a quanto avviene negli episodi di *phishing* e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario.

Il Collegio riconosce, dunque, un concorso di colpa tra le parti in relazione alle operazioni contestate e, nell'applicare l'art. 1227 c.c., accerta il diritto di parte ricorrente al rimborso della somma omnicomprensiva di € 9.000,00, determinata in via equitativa.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma onnicomprensiva di euro 9.000,00, 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