Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) MEZZACAPO	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO ACCETTELLA

Seduta del 13/12/2022

FATTO

1. L'odierno ricorrente sostiene di essere titolare del c/c n. ***505, al quale si appoggiano la carta di credito n. ***907 e una carta di debito. Afferma di aver ricevuto, il 14/04/2022, un sms, che si inseriva nel canale di comunicazione ufficiale con l'intermediario e che, con un pretesto, lo invitava a cliccare su un *link*. Il ricorrente nega di aver dato seguito al messaggio. Afferma di essere stato contattato, poco dopo, da un numero fisso riconducibile al servizio clienti dell'intermediario. Osserva che il sedicente operatore precisava che risultavano dei bonifici con beneficiario estero e chiedeva conferma di dette disposizioni di pagamento. Sostiene che, nel corso della conversazione, l'operatore chiedeva conferma di precedenti movimenti che il ricorrente aveva effettivamente effettuato nei giorni passati, così dimostrando di avere già accesso ai movimenti del conto corrente. Rileva che l'operatore, dopo aver consigliato di cancellare l'applicazione dal cellulare, dichiarava di aver provveduto a stornare i bonifici e riferiva che le operazioni di ristrutturazione dell'*home banking* erano già in corso, dando appuntamento telefonico per il giorno seguente per la definizione del problema. Parte ricorrente sostiene che, effettivamente, pervenivano, quasi contestualmente, i messaggi attestanti gli ordini di bonifico per euro 3.690,00 ed euro 3.450,00 e i relativi messaggi di storno. Afferma di aver ricevuto, altresì, il messaggio che confermava l'appuntamento telefonico con l'operatore per il giorno seguente alle ore 9:30. Sostiene di aver poi ricevuto, il 15/04/2022, la

telefonata dal numero verde e osserva che il sedicente operatore confermava che erano in corso le necessarie operazioni di bonifica del conto corrente. Aggiunge di aver ricevuto, quindi, altri due messaggi attestanti due nuove disposizioni di bonifico di importo pari, rispettivamente, a euro 2.800,00 ed euro 1.480,00, con i correlati immediati messaggi di storno. Il ricorrente sostiene ancora che, in data 19/04/2022, il truffatore lo contattava ancora una volta e riferiva che le operazioni non erano ancora concluse, anticipando un nuovo contatto per il giorno successivo e l'eventuale necessità di un appuntamento presso la filiale. Osserva di aver ricevuto, il successivo 20/04/2022, un ulteriore messaggio attestante la disposizione di bonifico internazionale di euro 2.250,00 e la relativa immediata comunicazione di storno. Afferma di aver ricevuto altresì, il 21/04/2022, alle ore 14:00 circa, una nuova telefonata dal numero verde, con la quale un operatore gli comunicava la possibilità di definire le problematiche riscontrate tramite telefono e, contestualmente, quattro email e un altro sms, sempre sulla *chat* ufficiale, con i quali gli venivano indicati alcuni codici di attivazione dell'*app*. Afferma che l'operatore richiedeva la comunicazione dei predetti codici telefonicamente e sosteneva che, per riattivare il conto, fosse necessario effettuare un bonifico sul conto ***2505 o un'operazione con la carta di credito. Il ricorrente, insospettitosi, contattava il servizio clienti dell'intermediario convenuto e scopriva di essere stato vittima di truffa. Oltre ai cinque bonifici, disconosce un'operazione effettuata con carta di credito di euro 600,00. Parte ricorrente osserva che, recatosi in filiale, un addetto lo rassicurava sul fatto che tale operazione risultava ancora "in corso di autorizzazione" e sarebbe stata stornata, ma rileva che ciò non è avvenuto, posto che il relativo importo è stato addebitato sul conto il mese successivo. Il ricorrente nega di aver ricevuto un messaggio di attivazione dell'*app* il 14/04/2022. Ravvisa una grave compromissione del sistema informatico della banca. Ritiene di essere rimasto vittima di una frode sofisticata. Osserva che l'onere di provare la corretta autenticazione delle operazioni disconosciute e la colpa grave del cliente incombe sull'intermediario e che la banca non ha rilevato il carattere anomalo delle operazioni (cinque bonifici esteri per l'importo complessivo della giacenza presente sul conto), omettendo l'adozione di adeguati sistemi di monitoraggio.
Parte ricorrente chiede il rimborso, anche a titolo di risarcimento danni, della somma di euro 14.275,00, oltre interessi legali, nonché delle spese.
2. L'intermediario resistente, con le proprie controdeduzioni, rileva che l'accesso alle funzioni di *inquiry* e dispositive avviene tramite un sistema con autenticazione forte. In particolare, l'accesso alla *HB* da *App* prevede: - per effettuare il *login* e le operazioni di *inquiry*, l'inserimento del numero cliente + PIN e il codice OTP, codice dinamico generato da *Mobile Token*; - per disporre le operazioni, l'inserimento del PIN e della OTP generata da *Mobile Token.* L'attivazione del *Mobile Token* è possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via sms al numero di cellulare certificato. Parte resistente osserva che il cliente ha ricevuto alle ore 17:15 del 14/04/2022 un sms al numero di cellulare certificato n. ***373 dal seguente tenore: "Stai attivando Mobile Token. Ricordati che il personale *** non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: *******". Parte resistente sostiene di aver adottato un sistema di autenticazione forte. Rileva che dai *log* risultano i seguenti passaggi: - alle ore 17:15 del 14/04/2022 è stato attivato il *Mobile Token* mediante inserimento del PIN e del codice OTP ricevuto via sms, con verifica a due fattori, utilizzando l'OTP generata dal *Mobile Token*; - alle ore 17:16 è stata visualizzata la rubrica; alle ore 17:19 e alle ore 17:22 sono stati inseriti due bonifici autorizzati con PIN e OTP generata da *Mobile Token* (rispettivamente, di euro 3.690,00 e di euro 3.450,00); il 15/04/2022, alle ore 17:36 e alle ore 17:40, sono stati inseriti altri due bonifici autorizzati con PIN e OTP generata da *Mobile Token* (rispettivamente di euro 2.800,00 e di euro

1.480,00); - il 20/04/2022 alle ore 10:07 è stato predisposto un altro bonifico (di euro 2.250,00) autorizzato con PIN e OTP generata da *Mobile Token*; il 21/04/2022 alle ore 14:14 è stato attivato il *Mobile Token* mediante inserimento del PIN e dell'OTP ricevuta via sms, con verifica a due fattori, utilizzando l'OTP generata dal *Mobile Token*; - il 21/04/2022 alle ore 14:30 è stata autorizzata tramite SCA la transazione internet con PIN e OTP generata da *Mobile Token*. Parte resistente precisa che il blocco della carta è avvenuto il 21/04/2022 alle ore 16:32. Afferma di aver inviato al numero di cellulare certificato, a fronte di ciascuna operazione dispositiva, la relativa notifica *push* e l'*sms alert*. Osserva che il ricorrente ha denunciato l'accaduto otto giorni dopo, impedendo alla banca di eseguire positivamente le procedure di *recall* almeno dei bonifici. Presume, pertanto, una colpa grave del cliente nella custodia delle credenziali, in presenza di un sistema di autenticazione forte. Ritiene che il cliente sia rimasto vittima di uno schema di frode classica, dal momento che il *link* contenuto nel messaggio civetta non è riconducibile alla banca. Osserva che, nel ricorso, il ricorrente nega di aver dato seguito all'sms esca, ma aggiunge che dalla relazione dell'ufficio antifrode del 21/04/2022 risulta che il ricorrente abbia confermato di aver inserito le sue credenziali nel *link* ricevuto il 14/04/2022. L'intermediario resistente sostiene di informare la propria clientela sui rischi di frodi informatiche. Chiede, pertanto, il rigetto del ricorso.

3. In sede di repliche, il ricorrente contesta le controdeduzioni e nega di aver ricevuto il 14 aprile 2022 un messaggio di attivazione del *Mobile Token* ("Invio codice attivazione Mobile Token"), come risulta dalle schermate prodotte in allegato alla denuncia-querela del 21 aprile 2022 e come emerge dall'elenco degli sms prodotti dalla stessa banca ove non è presente detto sms (14 aprile 2022, ore 17:15). Il ricorrente afferma di non aver comunicato il codice OTP a nessuno (come invece asserisce la banca), proprio perché, prima dell'esecuzione dei cinque bonifici in contestazione, non ha mai ricevuto alcun messaggio di attivazione del *Mobile Token*, né alcun codice OTP. Aggiunge che dalla documentazione della banca risulta che il *Mobile Token* è stato attivato da un'utenza telefonica diversa da quella del ricorrente titolare del conto. Ribadisce il carattere anomalo delle operazioni e contesta la relazione dell'ufficio antifrode, peraltro non prodotta in atti. Rimarca di essere stato vittima di truffa sofisticata, che esclude la sua colpa grave. Ribadisce di aver ottenuto rassicurazioni dalla banca in merito al fatto che l'operazione con carta di credito risultasse ancora "in corso di autorizzazione" e sarebbe stata stornata. Osserva che ciò non è avvenuto, posto che il relativo importo è stato addebitato sul conto il mese successivo.

DIRITTO

1. Le operazioni di pagamento fraudolente contestate da parte ricorrente, consistenti in cinque bonifici e un'operazione *online* disposta con carta di credito, ammontano complessivamente a euro 14.275,00 e sono state effettuate tra il 14/04/2022 e il 21/04/2022. Esse, dunque, risultano compiute dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (cosiddetta *PSD 2 - Payment Services Directive* 2), recepita con il d.lgs. n. 218 del 15/12/2017, entrato in vigore in data 13/01/2018, che modifica in più punti il d.lgs. n. 11 del 2010.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede che "le misure di sicurezza di cui agli articoli 5-*bis*, commi 1, 2 e 3, 5-*ter*, 5-*quater* e 10-*bis* del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della

direttiva – ha emanato il 27/11/2017 il regolamento delegato (UE) n. 2018/389 *che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri*. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14/09/2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13/03/2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14/09/2019 e risultano dunque applicabili nel caso in esame.

2. La nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte". Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-*bis*, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-*bis* dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

Il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-*bis*) d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "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 concetto è ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, dall'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019.

3. Qualora il prestatore di servizi di pagamento abbia adottato un sistema di autenticazione forte del cliente, si ricade nelle fattispecie regolate dai commi terzo e quarto dell'art. 12 d.lgs. n. 11/2010. In base al primo, "salvo se abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'articolo 7, con dolo o colpa grave, il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate derivanti dall'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita". Mentre, ai sensi del secondo, "qualora abbia agito in modo fraudolento o non abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave, l'utente sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3". A sua volta, l'art. 7 del decreto prevede gli obblighi che l'utente dei servizi di pagamento deve osservare in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate. In particolare, il comma primo, lett. a) impone a costui di "utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso", mentre il comma secondo dispone che, ai fini del corretto utilizzo dello strumento di pagamento, "l'utente, non appena riceve uno strumento di pagamento, adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate". Il Provvedimento della Banca

d'Italia del 5/07/2011 di *Attuazione del Titolo II del decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti)* ribadisce e precisa le suddette previsioni normative.
Va altresì richiamata la previsione dell'art. 10, comma 1, d.lgs. n. 11/2010 [così come introdotto dall'art. 2, comma 10, lettera c) d.lgs. n. 218/2017], in relazione alla *prova di autenticazione ed esecuzione delle operazioni di pagamento*: "Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già 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 comma secondo della medesima norma precisa che: "Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente 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. 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".
4. Nel caso di specie, la truffa subita dal ricorrente sembra riconducibile a un episodio di *smishing*, combinato al *vishing*. Il ricorrente dichiara infatti di aver ricevuto un sms dal numero dell'intermediario, il quale lo avvertiva della necessità di aggiornare i propri dati sull'*App*. Il ricorrente afferma di non aver dato seguito al messaggio e nonostante ciò di essere stato contattato poco dopo da un sedicente operatore dell'intermediario resistente.
5. In relazione alle modalità di autenticazione delle operazioni di pagamento contestate, l'intermediario resistente afferma che esse risultano regolarmente autenticate, registrate e contabilizzate. Osserva che l'accesso alle funzioni di *inquiry* e dispositive avviene tramite un sistema con autenticazione forte. In particolare, l'accesso alla *Home Banking* da *App* richiede, per effettuare il *login* e le operazioni di *inquiry*, l'inserimento del numero cliente, del PIN e del codice OTP, codice dinamico generato da *Mobile Token*. Per disporre le operazioni, queste ultime devono essere poi confermate con l'inserimento del PIN e della OTP generata dal *Mobile Token*.
In merito alla fase di attivazione del *Mobile Token*, i Collegi territoriali dell'ABF sono soliti evidenziare la necessità dell'adozione di un sistema di autenticazione a doppio fattore non solo per le operazioni dispositive, ma anche per la variazione del *device*.
Nel caso di specie, come anticipato, l'intermediario rileva che l'attivazione del *Mobile Token* è possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente e PIN) e del codice OTP inviato al cliente via sms al numero di cellulare certificato. In particolare, dai dai *log* prodotti dall'intermediario risulta che il 14/04/2022 alle ore 17:15 è stato attivato il *Mobile Token* mediante inserimento del PIN e di un codice OTP, con verifica a due fattori. L'intermediario afferma che l'OTP è stata inviata tramite sms al numero di cellulare certificato ***373 e produce una schermata dalla quale si evince che il numero di cellulare corrisponde a quello indicato dal cliente sul modulo di ricorso all'ABF.
6. Quanto alle operazioni contestate, sulla base della documentazione versata agli atti, i bonifici risultano effettuati da *App* tra il 14 e il 20/04/2022, con inserimento del PIN e dell'OTP, generata dal *Mobile Token*.
In dettaglio, il 14/04/2022 alle ore 17:19 e alle ore 17:22 risultano autorizzati due bonifici, rispettivamente, di euro 3.690,00 e di euro 3.450,00. Il 15/04/2022 alle ore 17:30 risulta effettuato il *login* mediante inserimento del PIN e dell'OTP generata dal *Mobile Token*.

Successivamente sono stati inseriti altri bonifici disconosciuti, autorizzati con PIN e OTP generata dal *Mobile Token*. Infine, il 21/04/2022, alle ore 14:14, è stato attivato il *Mobile Token* mediante inserimento del PIN e utilizzando l'OTP ricevuta via sms, con verifica a due fattori. Successivamente, alle ore 14:30, è stata autorizzata la transazione internet con PIN e OTP generata dal *Mobile Token*.

Da quanto sopra rilevato, si evince che l'intermediario adotta, per le operazioni di *internet banking*, un sistema di autenticazione basato sull'utilizzo del *Mobile Token* integrato nell'*App*, che genera una OTP (fattore di possesso), in seguito all'inserimento di un PIN. E questo Collegio ha già ritenuto *compliant* alla SCA una simile modalità autorizzativa (cfr. Collegio di Roma, decisione n. 19821/2021).

Dai suddetti elementi di fatto, può dunque ritenersi che l'intermediario resistente abbia soddisfatto l'onere della prova richiesta dall'art. 10 d.lgs. n. 11/2010 in merito all'autenticazione e alla corretta registrazione e contabilizzazione delle operazioni di pagamento contestate dal ricorrente.

7. Il rilevo del ricorrente in base al quale il carattere anomalo delle operazioni avrebbe dovuto allertare la banca non è condivisibile.

In effetti, né la circostanza che i cinque bonifici fossero esteri né il fatto che l'importo complessivo degli stessi fosse quasi corrispondente alla giacenza presente sul conto corrente del cliente costituiscono indici sintomatici di un rischio di frode in base alle previsioni del d.m. 30 aprile 2007, n. 112, adottato in attuazione della legge 17 agosto 2005, n. 166, recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento".

8. Quanto alla condotta del ricorrente, nella veste di utente del servizio di pagamento, va rilevato che il Collegio di Coordinamento, con la decisione n. 22745/2019, ha enunciato il seguente principio di diritto: "*la previsione di cui all'art. 10, comma 2, del 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 a 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*". Ha, tuttavia, precisato anche che, "*nel caso in cui l'intermediario si sia costituito nel procedimento, fornendo prova dell'autenticazione e della regolarità formale dell'operazione, ma nulla abbia dedotto in merito alla colpa grave dell'utente, il Collegio possa comunque affermarne l'accertamento se palesemente emergente dalle dichiarazioni rese dal ricorrente in sede di denuncia all'autorità giudiziaria e/o nel ricorso*".

9. Nel caso di specie, è lo stesso ricorrente a dichiarare di aver ricevuto un sms truffaldino, contenente un *link*, sebbene egli neghi di aver dato seguito al messaggio.

Sulla base delle affermazioni rese dalla parte ricorrente e della documentazione presente in atti, si può ritenere che la truffa si sia svolta secondo le modalità tipiche del c.d. *spoofing*. Si tratta di 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).

Come già evidenziato, il ricorrente ha infatti fornito evidenza del messaggio ricevuto, che si è inserito nel canale di comunicazione ufficiale con l'intermediario resistente.

10. Il Collegio di Coordinamento, nella citata decisione n. 22745/2019, ha dato conto di tale tipologia di frode, già segnalata nel *Report* pubblicato in data 01/12/2018 dall'*European Payments Council*. In particolare, il Collegio ha rilevato che "*appare significativa la segnalazione da parte degli stessi organismi gestori dei servizi di*

pagamento di possibili intrusioni truffaldine tramite «Messaggi SMS "spoofed"», attraverso i quali gli aggressori utilizzano dei software per modificare l'ID del mittente del messaggio in modo che appaia con il nome del PSP. In sostanza, il messaggio truffaldino verrebbe visualizzato negli smartphone insieme a precedenti messaggi legittimi provenienti effettivamente dal PSP, aumentando la probabilità che il messaggio stesso venga considerato genuino (segnalazione tratta da "2018 Payment Threats and Fraud Trends Report", pubblicato in data 1/12/2018 dall'European Payments Council (EPC)). Inoltre, va rilevato che, nella casistica dei ricorsi esaminati dall'Arbitro, si rinvengono svariate ipotesi di intrusioni sofisticate, come, ad esempio, modifiche della linea telefonica associata agli strumenti di pagamento o installazione di App dell'intermediario su un device diverso da quello del ricorrente, escludendo in tal modo il cliente dalla fase conclusiva di autorizzazione dell'operazione fraudolenta (ad es., cfr. le decisioni Coll. Bari nn. 7225/19, 14530/18, 14190/17, Coll. Roma n. 10125/18, Coll. Bologna n. 4564/18). (…)".

A queste ipotesi di frodi sofisticate sembra riconducibile anche quella di cui il ricorrente è rimasta vittima nel caso in esame.

Del resto, una differenziazione nei metodi attraverso i quali può realizzarsi la truffa informatica è chiaramente evidenziata dal Collegio di Coordinamento, già nella decisione n. 3498/2012, ove si afferma che, nei metodi "tradizionali" di *phishing* (o di *smishing*), "*il cliente è vittima di una colpevole credulità [in quanto] portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di Internet; nel caso che ci occupa, invece, il subdolo meccanismo di aggressione ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino*".

In casi come quelli appena enunciati appare invocabile anche l'art. 8, comma 1, d.lgs. n. 11/2010, ai sensi del quale "il prestatore di servizi di pagamento che emette uno strumento di pagamento ha l'obbligo di: a) assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento". Si tratta di un obbligo a contenuto organizzativo gravante in capo all'intermediario, a sua volta precisato dal già richiamato Provvedimento attuativo della Banca d'Italia del 5/07/2011.

11. Secondo la più recente posizione condivisa dai Collegi territoriali dell'ABF, 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; in tale caso, potrà essere ravvisato 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).

Alla luce di un simile orientamento, si osserva che, nella vicenda in esame, il testo del messaggio "esca" contiene un evidente errore grammaticale e fa riferimento a un *link* non riconducibile all'intermediario resistente. Vi sono dunque indici di anomalia nel messaggio, che avrebbero dovuto indurre il cliente a nutrire almeno un dubbio sulla genuinità dello stesso e che questo Collegio ha già avuto modo di ritenere rilevanti ai fini della prova della colpa grave della parte ricorrente (cfr. Collegio di Roma, decisione n. 2277/2021 e decisione n. 1625/2022).

12. Va anche rilevato, tuttavia, che il ricorrente nel caso in esame ha ricevuto – subito dopo il messaggio parlante (genuino) – un sms di conferma dell'avvenuto storno dell'operazione, che può aver rafforzato l'affidamento dell'utente circa la correttezza della procedura. Nei casi di frodi particolarmente sofisticate si è infatti ritenuto che il messaggio che indica il successivo avvenuto storno, sempre ricevuto dal numero dell'intermediario, possa attenuare l'efficacia del precedente messaggio c.d. "parlante" (si veda in tal senso la decisione recentemente assunta per un caso simile dal Collegio di Torino, n. 457 del 10 gennaio 2022).
13. Tenuto conto di tutti i 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 del cliente, per i danni derivanti dal compimento delle operazioni di pagamento non autorizzate e dispone che l'intermediario corrisponda alla parte ricorrente l'importo di euro 10.000,00, a titolo di risarcimento del danno determinato in via equitativa.
14. Va invece respinta la richiesta di parte ricorrente di rimborso delle spese, giacché non è stata versata agli atti alcuna parcella o altra documentazione analoga al fine di dare conto delle spese sostenute.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 10.000,00, determinata in via equitativa. Respinge nel resto.
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