COLLEGIO DI ROMA

composto dai signori:

(RM) MARINARO	Presidente
(RM) ACCETTELLA	Membro designato dalla Banca d'Italia
(RM) PORTA	Membro designato dalla Banca d'Italia
(RM) GENOVESE	Membro di designazione rappresentativa degli intermediari
(RM) CHERTI	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO ACCETTELLA

Seduta del 18/11/2021

FATTO

1. L'odierno ricorrente riferisce di aver ricevuto, in data 06.10.2020, alle ore 13:56, un sms dal numero 06**60, corrispondente al Servizio Clienti dell'intermediario convenuto, dal seguente tenore: "Gentile Cliente le sue utenze saranno limitate per mancanza di sicurezza web. Le aggiorni https://certificazioneanagrafica .com/". Confidando nella genuinità del messaggio, ha cliccato sul *link* aprendo una pagina web in tutto simile al sito dell'intermediario, in cui, dopo avere immesso le credenziali di accesso al conto corrente, ha effettuato – come richiesto – la procedura di aggiornamento dei dati anagrafici. Sostiene che la procedura si è conclusa con un secondo sms che preannunciava la telefonata di un operatore della banca. Afferma di aver ricevuto, alle ore 17:46, una telefonata dal medesimo numero, nel corso della quale il sedicente operatore, allo scopo dichiarato di aggiornare i dati anagrafici, lo ha indotto a dettare la sequenza numerica nel frattempo pervenuta tramite sms delle ore 17:47. Aggiunge di aver ricevuto, alle ore 19:13, n. 3 sms di notifica dell'avvenuta esecuzione di altrettanti bonifici di importo pari, rispettivamente, a euro 6.000,00, a euro 6.100,00 e ad euro 8.100,00, e, complessivamente, di ammontare corrispondente all'intero saldo del conto corrente, pari a euro 20.200,00. Alle ore 19:27 ha contattato il servizio clienti dell'intermediario al medesimo numero 06**60, disconoscendo i bonifici e chiedendo l'immediato blocco del conto. Esperito infruttuosamente reclamo, il ricorrente in data 16.12.2020 ha presentato istanza di mediazione, conclusasi con esito negativo per la mancata partecipazione della banca. Nelle more, l'intermediario ha proposto di definire la controversia con il rimborso della somma di euro 10.100,75, ritenuta incongrua.

Parte ricorrente sostiene che la frode è ascrivibile alla mancata adozione da parte dell'intermediario di adeguate misure di protezione idonee a garantire la sicurezza dei servizi offerti e al fatto che la banca ha consentito a terzi di violare il sistema informatico e di acquisire i dati personali del correntista. Aggiunge che i frodatori hanno potuto utilizzare il numero telefonico corrispondente al Servizio Clienti della banca traendolo così in inganno. Rileva inoltre che l'esistenza di soluzioni tecniche volte a realizzare la sostituzione del numero del mittente non costituisce un'esimente per l'istituto di credito, ma anzi un'aggravante, perché, nonostante la tecnologia sia da tempo nota, la banca non ha adottato le opportune precauzioni volte a evitarne l'uso fraudolento a danno dei correntisti. Sostiene ancora che l'intermediario non ha predisposto un adeguato sistema di monitoraggio volto a segnalare e eventualmente bloccare le disposizioni di pagamento anomale e che, nel caso di specie, si tratta di tre bonifici elettronici istantanei, effettuati in rapida successione, per un ammontare pari al saldo del conto di euro 20.200,00. Contesta il fatto che l'intermediario non abbia messo a disposizione la possibilità di apporre limitazioni alle operazioni di bonifico *online*, che avrebbero consentito di limitare gli effetti dannosi della frode. Lamenta poi che la mancanza di idonee misure di controllo ha consentito agli autori della truffa di generare il codice autorizzativo, carpito al correntista e necessario a creare un secondo *token* su un *device* in loro uso, con il quale hanno successivamente generato i codici dispositivi dei singoli bonifici. Rileva che la creazione del secondo *token* non è stata presidiata dall'invio di un *sms alert* o da altra idonea misura di verifica che avrebbe consentito al cliente di avvedersi della truffa e di disporre il blocco.
Parte ricorrente chiede quindi il rimborso della somma complessiva di euro 20.200,00, oltre alla rifusione delle spese legali, quantificate in euro 1.200,00.
2. L'intermediario resistente, con le proprie controdeduzioni, osserva che le transazioni disconosciute consistono in tre bonifici, disposti mediante *App* di *home banking*, per un importo complessivo di euro 20.201,50. Rileva che i servizi di *home banking* predisposti dall'intermediario prevedono un sistema di autenticazione "forte" con l'inserimento delle credenziali di accesso (numero cliente + PIN noto solo al cliente) per effettuare il *login*, e del PIN + *One Time Password* (OTP) per disporre le operazioni. Aggiunge che, nell'operatività da sito web, il codice OTP viene autorizzato tramite la notifica *push* su *smartphone* (o *tablet*), sulla quale il cliente deve cliccare e inserire il suo codice PIN o utilizzare i meccanismi *touchID* o *faceID*, mentre, in caso di operazioni dispositive, l'operazione di pagamento inserita viene confermata con il sistema della notifica *push* + PIN o mediante dati biometrici, che generano il codice OTP autorizzativo in modo silente, tramite il *Mobile Token* integrato nell'*App*. Osserva ancora che l'attivazione del *Mobile Token* – ossia del dispositivo digitale preposto a generare OTP direttamente dallo *smartphone* dell'utente – è possibile soltanto attraverso l'inserimento delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato via sms al cellulare collegato all'*home banking* e che il cliente può attivare n. 2 *Mobile Token* su altrettanti dispositivi diversi, mentre non è possibile attivare sullo stesso *device* più di un *Mobile Token*. Parte resistente rileva che, nel caso specifico, il *Mobile Token* è stato attivato sul *device* del frodatore in data 06.10.2020, mediante inserimento delle credenziali di sicurezza e del codice OTP inviato via sms al cellulare del ricorrente e da questi dettato al finto operatore telefonico. Aggiunge che il testo dell'sms era il seguente: "Stai attivando il Mobile Token. Ricordati che il personale [dell'intermediario] non te lo chiederà mai, quindi NON COMUNICARE A NESSUNO il codice riservato: ******** Info ******". Osserva che, a fronte di un simile messaggio, il ricorrente, anziché contattare immediatamente la banca, è rimasto inerte. Afferma inoltre che la truffa è stata perpetrata mediante uno schema di *phishing* ormai noto, che non costituisce una truffa sofisticata, come da ormai consolidato orientamento dell'ABF. In particolare, sostiene che, con le credenziali di sicurezza

comunicate colpevolmente dal titolare, il frodatore è stato in grado di accedere all'*App* di *home banking* a nome del cliente e ha avuto accesso a tutti i suoi dati personali e bancari. Rileva che il sistema di autenticazione "a due fattori" adottato dall'intermediario è riconosciuto come un sistema "forte" anche dall'orientamento diffuso dei Collegi territoriali dell'ABF e che dall'esame dei *log* allegati emerge che le operazioni sono state correttamente autenticate, registrate e contabilizzate senza alcun malfunzionamento del sistema operativo della banca. Afferma ancora che il ricorrente ha tenuto una condotta gravemente colposa e inescusabile, in violazione degli obblighi di custodia e protezione delle credenziali di sicurezza personalizzate dei suoi strumenti di pagamento, per avere confidato nell'attendibilità del messaggio esca, nonostante tale forma di truffa sia ormai nota e sia oggetto di un'ampia campagna informativa e preventiva da parte dell'intermediario. Infine, sostiene che non è dovuto il rimborso delle spese legali, considerato il carattere non necessario dell'assistenza tecnica per il procedimento ABF.
Parte resistente chiede pertanto il rigetto del ricorso.
3. In sede di repliche, il ricorrente contesta il contenuto delle controdeduzioni, rilevando che l'intermediario ha preso più volte visione, per il tramite di propri funzionari, dell'sms esca, riportato nel verbale di denuncia-querela, allegato al ricorso introduttivo. Osserva che la pronuncia del Collegio di Roma, richiamata dalla banca resistente, non specifica con quale mezzo il ricorrente debba fornire la prova del messaggio civetta. Ne ricava che il correntista può fornire evidenza di tale messaggio con ogni mezzo, compresa la denuncia-querela nella quale il messaggio in questione è stato testualmente riportato nel suo contenuto, con responsabilità penale del denunciante per false dichiarazioni. Ove necessario, il ricorrente si rende disponibile a procurare alla banca i tabulati telefonici della propria utenza e a sottoporre a perizia il proprio dispositivo telefonico. Diversamente da quanto sostiene l'intermediario, parte ricorrente afferma che, per effettuare il *login* da sito web dell'intermediario, è necessario, oltre all'inserimento del codice cliente e del PIN, che il correntista autorizzi l'accesso, attraverso il proprio *smartphone*, cliccando sulla notifica-*push*, che il ricorrente sostiene di non aver mai ricevuto. Inoltre, sostiene che il falso operatore telefonico ha potuto telefonare dal numero 06**60 corrispondente al Servizio Clienti dell'intermediario, violandone la rete telefonica, e che, durante la chiamata, era già in possesso di tutti i dati anagrafici e personali del titolare e non solo del codice cliente e del PIN inconsapevolmente forniti. Rileva che il frodatore ha così potuto generare un codice OTP sullo *smartphone* del correntista, senza che questi ne abbia autorizzato l'accesso all'*home banking* con notifica *push* che avrebbe dovuto ricevere sul proprio *smartphone*. Aggiunge che attualmente l'intermediario invia al correntista un avviso di attivazione ogni qualvolta venga abilitato un nuovo *token* e che tale precauzione non era in uso all'epoca dei fatti. Precisa che le spese legali si sono rese necessarie per la promozione del tentativo di mediazione e per il comportamento ostruzionistico dell'intermediario. Insiste quindi per l'accoglimento del ricorso.

DIRITTO

1. Le operazioni di pagamento *online* disconosciute dal ricorrente sono state eseguite in data 06.10.2020. Risultano pertanto effettuate 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 tuttavia 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.
Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.
2. In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un cd. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). 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".
3. Orbene, 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 oggi 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.
4. 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.

5. 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".

6. Nel caso di specie, le operazioni contestate consistono in n. 3 bonifici, disposti tramite l'*App* di *home banking* dell'intermediario convenuto per un importo totale di euro 20.201,50.

In relazione alle modalità di autenticazione delle operazioni disconosciute, l'intermediario ha prodotto documentazione tecnica comprovante l'autenticazione a doppio fattore in fase di accesso all'*App* e in fase di autorizzazione dei bonifici. Nello specifico, dai *log* prodotti si evince che il frodatore ha, dapprima, attivato il *Mobile Token* con nickname "hdhdhdhd" mediante inserimento del PIN e dell'OTP ricevuto via sms, nonché mediante verifica a due fattori, realizzata tramite l'OTP generata da *Mobile Token*. Ha poi effettuato il *login* con il proprio *device*, mediante inserimento del PIN e, anche qui, mediante verifica a due fattori, tramite l'OTP generata dal *Mobile Token.* Ha infine inserito i bonifici fraudolenti, autorizzati mediante *Strong Customer Authentication*, in particolare tramite PIN e OTP generata da *Mobile Token*.

Questo Collegio ha già avuto modo di ritenere – sulla scia dell'*Opinion* dell'EBA sopra richiamata – che la modalità autorizzativa che fa leva sull'inserimento di credenziali statiche (per esempio, il PIN) e del codice OTP generato da un *Mobile Token* (per esempio una *Token App*) sia *compliant* rispetto alla SCA (così Collegio di Roma, decisione n. 6634/2021).

Dalla documentazione in atti può dunque ricavarsi la vigenza, per le transazioni *online* e, in particolare, per quelle oggetto di contestazione, di un sistema di sicurezza a due fattori e dell'accessibilità dello stesso solo al cliente, con la conseguenza di ritenersi assolto l'onere della prova richiesta dall'art. 10 d.lgs. n. 11/2010 in merito all'autenticazione e alla corretta registrazione delle operazioni contestate.

7. In relazione 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*".

8. Sulla base delle affermazioni delle parti e della documentazione in atti, la truffa si è svolta secondo le seguenti modalità. In data 06.10.2020, alle ore 13:56, il cliente ha ricevuto un sms, proveniente dal numero dell'intermediario e inserito in una precedente conversazione genuina, contenente un *link* per effettuare l'aggiornamento di sicurezza delle utenze *web*. Il cliente afferma di aver aperto il *link* e di aver inserito nella pagina – apparentemente uguale a quella dell'intermediario – le credenziali di accesso al conto corrente richieste dal sistema. Alle ore 17:46 è stato contattato sul proprio di cellulare da un numero corrispondente a quello del Servizio Clienti dell'intermediario, che aveva salvato in rubrica. Il ricorrente riferisce, infine, che, a conclusione della telefonata, alle ore 17:52, ha richiamato il medesimo numero per sincerarsi della provenienza della chiamata ricevuta e produce lo *screenshot* della lista delle chiamate intercorse con l'utenza in questione, dal quale risultano entrambe le chiamate (una in entrata e una in uscita). Nel corso della telefonata, il ricorrente ha comunicato al proprio interlocutore il codice OTP ricevuto via sms, che è servito per attivare il *Mobile Token* dei frodatori. Qualche ora dopo la telefonata, tra le ore 19:13 e le ore 19:17, sono stati eseguiti, in rapida successione, i tre bonifici istantanei fraudolenti, comunicati al titolare del conto mediante *sms alert*.

Orbene, appare significativo che – come si ricava dalla schermata versata dal ricorrente agli atti del presente procedimento – il messaggio truffaldino sia stato visualizzato dal ricorrente nella stessa videata dove compaiono i messaggi legittimi provenienti effettivamente dal suo prestatore di servizi di pagamento, generando così nell'utente un legittimo affidamento circa la genuinità (anche) del messaggio fraudolento. Inoltre, per un verso, non si rinvengono evidenti indici di inattendibilità o anomalia del predetto messaggio, anzi il *link* in esso contenuto è preceduto dal protocollo di sicurezza più evoluto *https://*; per altro verso, l'affidamento del ricorrente sulla genuinità dell'sms risulta rafforzato dalla somiglianza tra la vera pagina *web* di accesso all'"area clienti privati" della banca resistente e quella falsa, nonché dalla successiva telefonata ricevuta dal numero verde della banca, ad opera di un sedicente operatore della stessa.

9. 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 1.12.2018 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 rimasto 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*" (nello stesso senso v. anche Collegio di Milano, decisione n. 22556/2019; Collegio di Roma, decisione n. 511/2015). 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.

A giudizio di questo Collegio, nella vicenda in esame l'intermediario non ha dunque fornito la prova della frode, del dolo o della colpa grave dell'utente, richiesta dall'art. 10, comma 2, d.lgs. n. 11/2010 (per la medesima conclusione, con riferimento a vicende analoghe a quella in esame, Collegio di Roma, decisioni n. 8534/2021, n. 3750/2021, n. 2414/2020, n. 16750/2020 e n. 26225/2019).

10. Alla luce dei suddetti elementi di fatto e tenuto conto delle previsioni richiamate del d.lgs. n. 11 del 2010, si deve ritenere che la responsabilità delle operazioni di pagamento oggetto di contestazione gravi sull'intermediario e che parte ricorrente abbia diritto ad ottenere il rimborso dell'importo complessivo ad esse corrispondente, al netto della franchigia di cui all'art. 12, comma 3, d.lgs. 11/2010.

11. In merito alla domanda di rimborso delle spese di assistenza professionale, quantificate in euro 1.200,00, il Collegio osserva che il ricorrente non fornisce evidenza del fatto che analoga domanda sia stata proposta nel reclamo del 29.10.2020, in quanto quest'ultimo non è stato prodotto agli atti. Peraltro, nelle lettere del 18.12.2020 e del 23.02.2021, trasmesse all'intermediario nell'ambito della trattativa per la soluzione bonaria della controversia, non risulta formulata richiesta di rimborso delle spese legali.

Al riguardo, le *Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari*, emanate dalla Banca d'Italia, stabiliscono (Sez. VI, par. 1) che il ricorso sia preceduto da un reclamo preventivo all'intermediario, avente ad oggetto la stessa questione esposta nel ricorso. Dal momento che non è noto se la suddetta domanda sia stata proposta in sede di reclamo, essa non può dunque essere accolta. Come chiarito dal Collegio di Coordinamento con decisione n. 6174/2016, infatti, "*la rimborsabilità delle spese di assistenza professionale, trattandosi del ristoro di un pregiudizio subito dal ricorrente, esige la prova del danno e la dimostrazione*

che esso è stato causato da un comportamento illegittimo dell'intermediario soccombente […] Per quanto sopra detto in ordine alla natura pregiudizievole delle spese di assistenza professionale, si deve escludere che esse possano essere ritenute conseguenza immediata e diretta della medesima condotta dell'intermediario lamentata nel reclamo, per cui occorre che esse – a pena d'inammissibilità della relativa domanda – siano autonomamente e specificamente richieste anche nel medesimo".

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 20.151,50. 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
MARCO MARINARO