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) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MARCO MARINARO

Seduta del 29/02/2024

FATTO

Il ricorrente, per il tramite del proprio procuratore, riferisce che:
- è titolare di un c/c in essere presso la resistente;
- in data 13.07.2023, alle ore 18:13, riceveva una chiamata da parte di un sedicente operatore della banca che lo invitava ad effettuare alcuni aggiornamenti di sicurezza al fine di evitare la sospensione dell'account;
- la telefonata risultava provenire da un numero riconducibile alla resistente, ragione per la quale l'istante riponeva pieno affidamento nell'interlocutore che lo esortava ad avviare la procedura cliccando su un apposito link inviato, nel frattempo, tramite sms;
- anche l'sms *"si posizionava esattamente tra quelli provenienti dalla controparte*";
- successivamente, il sedicente operatore lo invitava ad accedere alla casella di posta elettronica al fine di verificare la "*ricezione di un'e-mail per l'attivazione "token software*";
- l'istante comunicava "*avventatamente*" all'interlocutore il codice di attivazione contenuto nella mail;
- alle ore 18:31 della medesima giornata il ricorrente veniva notiziato, sempre tramite e-mail, dell'inoltro di un bonifico istantaneo per l'importo di euro 12.000,00 a favore di un c/c intestato a soggetto sconosciuto con causale "*Regalo Comunione*".

Così ricostruita la vicenda, il ricorrente rileva che:

• il contratto originariamente sottoscritto tra le parti non prevedeva la facoltà di eseguire bonifici istantanei ragione per la quale "*l'esecuzione di questi pagamenti*" configura "*un inadempimento rispetto al contratto di mandato*";
• laddove la banca dovesse produrre una comunicazione di modifica unilaterale del contratto contesta da subito il "*difetto di prova della natura recettizia dell'atto*";
• a conferma del fatto che l'abilitazione al bonifico istantaneo avrebbe richiesto apposita informativa richiama decisione del Collegio di Coordinamento n. 15627/21;
• rileva, inoltre, la mancata attivazione del servizio di alert sempre in spregio a quanto statuito dal Collegio di Coordinamento secondo cui, *"fra i doveri di protezione dell'utente rientra l'onere di fornire il servizio di SMS alert (o servizi assimilabili), da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene*";
• peraltro, il plafond a disposizione del cliente nel periodo in questione veniva "*ampiamente superato*", se si considera che "*a memoria del reclamante*" il limite all'operatività sul conto risultava fissato ad euro 5.000,00;
• al fine di verificare tale ultimo punto chiede, quindi, che sia allegata copia del contratto a norma degli art. 117 e 119 t.u.b.;
• in ogni caso rileva, quale ulteriore profilo di responsabilità della Banca, l'aver "*acconsentito*" in uno "*strettissimo lasso di tempo…all'esecuzione di operazioni di ingentissimo importo*" non riscontrabili nell'operatività storica del conto;
• richiama le decisioni del Collegio di Coordinamento n. 24366/19 e n.22745/19;
• evidenzia infine che, diversamente a quanto di norma richiesto al fine di autorizzare operazioni di bonifico (ovvero il codice OTP generato da App a seguito del riconoscimento biometrico tramite impronta digitale), nel caso di specie il codice "*apparentemente comunicato dal reclamante al truffatore e contenuto nell'email oggetto "Attivazione token software*" si è rilevata condizione sufficiente a far partire la disposizione di pagamento;
• va esclusa peraltro la colpa grave in capo all'utente considerato che:
- la chiamata è pervenuta dal telefono ufficiale della filiale;
- l'sms si è posizionato tra quelli della banca;
- il link recava un "*nome a dominio assolutamente plausibile*".

Costituitosi l'intermediario ripercorre, preliminarmente, la vicenda chiedendo di rigettare le contestazioni avanzate dall'istante in quanto:
• è rimasto vittima di una truffa informatica ampiamente nota (ovvero "spoofing", perpetrato tramite tecniche di cd. ingegneria sociale) rispetto alla quale ha già da tempo attivato una mirata campagna informativa rivolta alla clientela;
• il sistema di Home Banking prevede, inoltre, la notifica in automatico di messaggi (in cui sono descritte dettagliatamente le richieste che il cliente non deve assecondare) di cui il cliente deve necessariamente prendere visione per poter accedere alle funzioni della propria area riservata;
• nel caso di specie, l'intermediario ha provveduto all'invio dei citati messaggi sia in data 08.05.2023 che in data 27.06.2023;
• i servizi di pagamento adottati dalla Banca sono conformi agli standard di sicurezza previsti dalla Regolamentazione europea, prevedendo dunque un doppio fattore di autenticazione;
• nello specifico per poter accedere al servizio di home banking ed effettuare operazioni dispositive, il cliente deve procedere all'attivazione del "token" previa installazione di apposita App. Una volta eseguita la procedura di installazione dell'applicazione, tramite l'inserimento delle proprie credenziali (username e password), si può successivamente, attivare la ** Pass Code in modo da ricevere le chiavi numeriche "usa e getta" (OTP) che consentono di accedere alla propria area ed usufruire dei servizi di Internet Banking;

• dall'analisi dei log è possibile verificare che la disposizione di pagamento contestata risulta autenticata, correttamente registrata e contabilizzata senza aver subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Nel dettaglio, veniva eseguita con il regolare inserimento delle credenziali (userid, password e codici autorizzativi) di esclusiva pertinenza del cliente;
• peraltro, all'esito delle verifiche effettuate sulla linea telefonica, il fornitore del servizio ha escluso la presenza di anomalie di natura tecnica sulla stessa.

Tanto premesso, rappresenta che:

• il servizio di bonifico istantaneo era espressamente previsto nel contratto di conto corrente sottoscritto dal cliente. Nello specifico, a pag. 2 della "Richiesta di apertura di conto corrente" il cliente ha sottoscritto la presa visione di vari documenti tra cui il cd. "Foglio Informativo" dove vengono descritte le caratteristiche del servizio. Tra l'altro, a pag. 4 del "Documento di sintesi" vengono indicati i costi del servizio;
• in ordine alla contestazione relativa all'inoperatività del servizio di sms alert, rappresenta che lo stesso non è mai stato opzionato dal cliente ma che, in ogni caso (come ammesso anche in sede di denuncia alle autorità) la banca ha inviato, mediante posta elettronica, le comunicazioni relative all'inoltro della richiesta di bonifico istantaneo;
• quanto alla contestazione concernente il superamento del plafond giornaliero rileva che il limite contrattualmente previsto è pari ad euro 20.000,00 quindi maggiore rispetto all'importo sottratto. Rappresenta, inoltre, che -in data 06.06.2022- il cliente aveva chiesto e ottenuto l'aumento del limite giornaliero fino ad euro 50.000,00;
• rileva, in ogni caso, la colpa grave dell'utente che "incautamente, ha fornito all'interlocutore le proprie credenziali di accesso all'area home banking (di natura estremamente riservata) nonché i codici - altrettanto riservati - per procedere all'autorizzazione delle operazioni".

Il ricorrente replica alle controdeduzioni, insistendo per l'accoglimento delle richieste formulate e chiarendo che:

• diversamente da quanto asserito da controparte il contratto allegato non risulta firmato digitalmente;
• invero, a seguito della "verifica del documento con un programma per l'esame della firma digitale" risulta che "il documento "non contiene firme";
• inoltre, "il link ed anche il messaggio che si è accodato a quelli ufficiali della banca non conteneva[no] delle frasi sgrammaticate (come detto dalla banca) e comunque riportava[no] correttamente i riferimenti della [banca] stessa".

In sede di controrepliche l'intermediario richiama quanto già affermato nelle precedenti difese rinnovando la richiesta di accoglimento delle conclusioni ivi rassegnate. Rileva, inoltre, che:

• a sostegno dell'asserita mancata previsione contrattuale della possibilità di eseguire bonifici istantanei, il ricorrente contesta la validità del contratto stesso, in quanto non risulterebbe firmato digitalmente;
• tale contestazione sarebbe inammissibile in quanto non avanzata né in sede di ricorso, dove il ricorrente era già in possesso della copia del contratto (fornita con la risposta al reclamo), né tantomeno in sede di reclamo ma sollevata, per la prima volta, in sede di repliche.

Tanto premesso, nel merito, aggiunge quanto segue:

• dalla schermata prodotta risulta che, ai fini della verifica della firma digitale apposta sul contratto, il ricorrente abbia utilizzato -in data 3.11.2023- l'applicazione "GoSign" che apparentemente ha fornito una risposta di "assenza di firme";
• tuttavia, premesso che parte ricorrente non ha fornito prova di aver posto all'esame dell'applicazione proprio il contratto in contesa, l'eccezione è comunque priva di

fondamento considerato che “ripetendo la stessa operazione con il medesimo applicativo, in data 22.11.2023, il sistema ha fornito la seguente indicazione “sono state verificate 14 firme sul documento (4 copie contratto)”;

• inoltre, nella schermata fornita dall’applicativo, cliccando il link “apri dettagli” (cfr. allegato 1), viene evidenziata nuovamente la presenza di 14 firme mostrando la lista delle singole verifiche e offrendo la possibilità di cliccare su ognuna di esse per confermare la presenza della firma apposta dal ricorrente, in data 04.04.2022, sul file pdf del contratto de quo (cfr. allegato 2);

• pertanto “selezionando su uno qualsiasi dei link di “verifica al giorno della firma”, l’applicativo riporta ad una maschera successiva (cfr. allegato 3) dove vi è la conferma dell’autenticità della firma selezionata (“1 documento verificato con successo”) e, cliccando su “report”, il sistema genera un certificato di conferma che la verifica dell’autenticità delle predette firme sia stata esitata con successo (cfr. allegato 4)”;

• ad ulteriore riprova della presenza della firma digitale, l’intermediario ha utilizzato anche un altro verificatore (cfr. allegato 5);

• rileva di aver attivato la propria campagna informativa, a partire dal mese di febbraio 2020, quindi in data antecedente a quella della truffa;

• quanto all’autenticazione dell’operazione nel contratto è indicato che, per accedere al Servizio di Internet Banking, occorre inserire i seguenti codici:

-Codice Identificativo Utente (c.d. “User ID”): fornito dalla Banca e non modificabile dal cliente;

-Password di Accesso (c.d. “PIN”): codice alfanumerico che solo il cliente conosce e può modificare;

-OTP Login: password generata da dispositivo **Pass Code o **token per accedere all’Area Riservata;

-OTP Dispositivo: password generata da dispositivo **Pass Code o **token per confermare gli ordini di pagamento disposti dal cliente.

• nel caso in esame il cliente, in fase di sottoscrizione del contratto, ha scelto, quale strumento di autenticazione, il dispositivo **Pass Code, vale a dire un software capace di generare OTP che vengono richiesti sia per accedere all’Area riservata dell’Internet Banking che per confermare le disposizioni di pagamento;

• analizzando il tracciato dei log è possibile verificare che l’operazione effettuata in data 13.07.2023, è stata eseguita con il regolare inserimento dei codici autorizzativi di esclusiva pertinenza del cliente;

• ed infatti “il bonifico di € 12.000,00 è stato “autorizzato” alle ore 18:31 (rigo 38, colonna K denominata “TIMESTAMPCHIAMATA”). Sempre al rigo 38, colonna O, denominata “DATI ZEB” è invece possibile rinvenire, tra l’altro, i dati identificati del conto corrente “RAP= 300107202002990”, del contratto di home banking “KTR= 9807211016824”, l’importo dell’operazione “IMPOPE=12.000,00”, le coordinate bancarie del destinatario del bonifico “IBAN= IE37SUMU99036510745717”, ma, soprattutto, è possibile rinvenire la sigla “SCAPSD2=S” che indica che la disposizione è stata eseguita secondo lo schema autorizzativo SCA (Strong Customer Authentication), prevista dalla normativa PSD2 sui sistemi di pagamento, dove il parametro “=S” conferma che è stata rispettata”;

• detti parametri risultano del tutto identici e conformi a quelli relativi alle disposizioni di bonifico, disposte e riconosciute dal cliente nei giorni precedenti alle operazioni contestate;

• al fine di agevolare la lettura allega una ‘legenda’ esplicativa dei codici riportati in detto tracciato;

• precisa, inoltre, che lo schema di autenticazione associato al profilo del ricorrente, individuato dalla sigla S44, prevede abilitazioni dispositive a tre fattori (PSW, OTP PIN e

OTP P) per “interfaccia PC internet” e per l’“interfaccia mobile”, entrambe riferite al software OTP avente numero seriale 0005249997716;

- lo schema S44 è riportato nel file log precisamente al rigo 32 colonna O “DATI ZEB” al momento in cui è avvenuto l’accesso all’home banking (“Login”) da cui è stata originata e autorizzata in stretta sequenza temporale la disposizione fraudolenta (cfr. righe dalla 32 alla 38 del tracciato log).

DIRITTO

1.- L’operazione di pagamento online disconosciuta dalla parte ricorrente è stata eseguita in data 13 luglio 2023. Risulta pertanto effettuata dopo l’emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. 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. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.
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 c.d. “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.
L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".
Alla luce di un simile orientamento, con riguardo alle operazioni successive al 14.09.2019, questo Collegio ritiene che l'inserimento dei dati della carta, al fine di dar corso alle operazioni di pagamento, non integri un idoneo fattore di autenticazione (così, per esempio, Collegio di Roma, decisione n. 8493/2020, decisione n. 15221/2021 e decisione n. 21761/2021).
4.- La controversia ha ad oggetto un'operazione di bonifico istantaneo dell'importo di euro 12.000,00.
L'intermediario afferma che l'operazione di pagamento risulta correttamente autenticata, registrata e contabilizzata e che non è emerso alcun malfunzionamento o compromissione dei sistemi.
Chiarisce, in particolare, che l'operazione è stata effettuata a mezzo internet banking e validata attraverso un sistema a doppio fattore, previa istallazione del token software -verosimilmente- sul device del frodatore.
Rileva che, per accedere al servizio di Internet Banking ed eseguire operazioni dispositive occorre inserire i seguenti codici:
- Codice Identificativo Utente (c.d. "User ID"): fornito dalla Banca e non modificabile dal cliente;
- Password di Accesso (c.d. "PIN"): codice alfanumerico che solo il cliente conosce e può modificare;
- OTP Login: password generata da dispositivo *** Pass Code o *** token per accedere all'Area Riservata;
- OTP Dispositivo: password generata da dispositivo *** Pass Code o *** token per confermare gli ordini di pagamento disposti dal cliente.

Nello specifico, in sede di sottoscrizione del contratto, il ricorrente ha scelto quale strumento di autenticazione, il dispositivo *** Pass Code, vale a dire un software capace di generare codici temporanei 'usa e getta' (OTP) richiesti sia per accedere all'Area riservata dell'Internet Banking che per confermare le disposizioni di pagamento.
Pochi minuti prima della disposizione di pagamento (autorizzata alla 18:31) il ricorrente riceveva la seguente mail contenente il codice dinamico necessario ad attivare il token software. Ammette di aver "avventatamente" comunicato il citato codice al sedicente operatore.
Alla luce di quanto riferito dall'intermediario l'attivazione sarebbe quindi avvenuta mediante inserimento del nome utente e della password [fattore di conoscenza] e del codice dinamico inviato all'indirizzo mail del cliente [fattore di possesso].

In base a quanto riferito dall'intermediario l'accesso al conto sarebbe avvenuto con inserimento di User Id e Pin [fattore di conoscenza] e OTP generata da Token [fattore di possesso].
Quanto all'operazione dispositiva l'intermediario rileva che il bonifico di euro 12.000,00 è stato autorizzato alle ore 18:31 (cfr. rigo 38 colonna K) secondo lo schema autorizzativo SCA, come evidenziato dalla presenza della sigla "SCAPSD2=S" (cfr. rigo 38 colonna O, denominata "DATI ZEB"). Allega legenda esplicativa dei log.
L'intermediario ha inoltre aggiunto che lo schema di autenticazione associato al profilo del ricorrente e al relativo contratto di home banking n. 980xxxxxx6824, individuato dalla sigla S44, prevede abilitazioni dispositive a tre fattori (PSW, OTP PIN e OTP P) per "interfaccia PC internet" e per l'"interfaccia mobile", entrambe riferite al software OTP avente numero seriale 0005xxxxx716.
Per riassumere, stando a quanto allegato dall'Intermediario, i fattori impiegati sarebbero i seguenti.
Per l'accesso, conseguente all'enrollment: elemento di conoscenza: UserID e PIN; elemento di possesso: OTP generata da Token.
Per le singole operazioni: elemento di conoscenza: UserID e PIN (mutuati dall'accesso); elemento di possesso: OTP generata da Token.
Si rileva che sulla base delle risultanze dei log informatici emerge che le operazioni disconosciute siano state autenticate con un sistema di autenticazione forte, tuttavia non è possibile riscontrare quali fattori siano stati in concreto utilizzati.
5.- Nel verbale di denuncia, la parte ricorrente ricostruisce le modalità della frode in modo analogo all'odierno ricorso.
Dalla ricostruzione fornita emerge che:
1) in data 13.07.2023, il ricorrente riceveva una telefonata - proveniente da un numero riconducibile al servizio clienti dell'intermediario - nel corso della quale un sedicente operatore (già a conoscenza dei suoi dati personali) lo invitava a eseguire una procedura di aggiornamento al fine di evitare la sospensione del suo account;
2) nel mentre riceveva sulla propria utenza telefonica un sms, proveniente dal canale di comunicazione normalmente utilizzato dalla convenuta, contenente il link di attivazione della procedura;
3) il ricorrente cliccava sul link ricevuto e inseriva le credenziali di accesso al proprio home banking;
4) successivamente, sempre su richiesta dell'operatore, accedeva alla propria casella di posta elettronica e gli comunicava il codice di attivazione nel frattempo ricevuto;
5) riceveva quindi una mail che lo informava dell'esecuzione di un bonifico di euro 12.000,00 a favore di un beneficiario sconosciuto.
La parte ricorrente ha prodotto in atti screenshot del messaggio ricevuto e del registro chiamate.
Il messaggio risulta provenire del canale di comunicazione normalmente utilizzato dall'intermediario. Non contiene errori grammaticali. Il link allegato al messaggio contiene riferimenti all'intermediario. Il messaggio è preceduto da un altro sms esca (che preannunciava la chiamata dell'operatore) e da un messaggio genuino di allerta sulle possibili frodi.
La parte ricorrente, a dimostrazione che la chiamata ricevuta provenisse da un numero riconducibile all'intermediario resistente, ha allegato una schermata internet.
Relativamente ai messaggi c.d. parlanti, hanno condiviso che l'adempimento da parte degli intermediari dell'obbligo di cui al punto A previsto dall'art. 5 degli RTS dell'EBA (comunicazione al pagatore dell'importo dell'operazione di pagamento e del relativo beneficiario) non costituisce di per sé prova della colpa grave del cliente, la quale dovrà

essere quindi desunta attraverso i consueti indici di anomalia. In particolare, con riferimento alle comunicazioni in apparenza provenienti dagli intermediari, che inducono il cliente ad abbassare la sua soglia di attenzione, i Collegi hanno convenuto che l'eventuale colpa grave del cliente è desumibile, ad esempio, dall'inequivoca non riconducibilità all'intermediario del link contenuto nel messaggio civetta nonché da evidenti errori grammaticali o di sintassi sempre contenuti nel messaggio civetta. Resta salva la possibilità di individuare, anche in questi casi, una responsabilità concorrente dell'intermediario.

6.- All'esito dell'esame istruttorio, ad avviso del Collegio nel caso di specie la parte ricorrente deve ritenersi essere rimasta vittima di una fattispecie delittuosa riconducibile al c.d. "sms spoofing".

Secondo l'orientamento condiviso fra i Collegi 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".

Pertanto, non sussistendo indici di inattendibilità o anomalie del messaggio tali da consentire di ritenere che cliente abbia tenuto una condotta gravemente colposa, la domanda restitutoria deve essere accolta (con esclusione della rivalutazione monetaria richiesta dal ricorrente che non è dovuta trattandosi di debito di valuta).

PER QUESTI MOTIVI

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 12.000,00 oltre interessi dalla richiesta al saldo.
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