COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) ACCETTELLA	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 - MARCO MARINARO

Seduta del 07/10/2024

FATTO

Il ricorrente, titolare di un conto di moneta elettronica con carta di credito in essere con la resistente e di un conto aperto presso altra banca riferisce che:
- in data 31.10.23 riceveva un SMS apparentemente proveniente dalla resistente che lo informava di un accesso anomalo sul proprio home banking e lo invitava a cliccare sul link fornito per disconoscere un'operazione che era stata effettuata;
- eseguiva le istruzioni dell'SMS e veniva contattato, attraverso il numero verde della banca del gruppo della resistente, da interlocutore che si qualificava come "operatore della resistente" che confermava che era stato effettuato un accesso anomalo sul conto del ricorrente e che era stato effettuato un tentativo di prelievo;
- invitava il ricorrente a spostare il proprio credito disponibile, pari ad € 517,00, tramite l'app della resistente;
- il ricorrente eseguiva le indicazioni ricevute dall'operatore;
- l'interlocutore, che era a conoscenza dell'altro conto da lui intrattenuto presso altra banca, lo invitava ad effettuare la medesima operazione "per precauzione", anche per la somma disponibile sull'altro conto (€ 4.500,00) attraverso bonifici dal conto alla carta della resistente, rassicurandolo poi sul ritorno del credito;
- solo successivamente, non ricevendo alcun rimborso, si rendeva conto di essere stato truffato e sporgeva denuncia il 31.10.2023, denuncia poi integrata il 2/11/2023 (cfr. infra);
- chiede il rimborso dell'importo sottratto, pari a € 5.008,00.

L'intermediario resiste al ricorso ed eccepisce quanto segue:
- il ricorrente conferma di avere eseguito personalmente le operazioni contestate, anche se dietro raggiro di un falso operatore. Pertanto, secondo l'orientamento generale dei collegi ABF, non si applica la disciplina delle operazioni di pagamento non autorizzate né i reciproci obblighi previsti dagli artt. 7 e ss. del d.lgs. 11/2010;
- il ricorrente non allega l'SMS all'origine della truffa subita, quindi, non è possibile analizzarne il testo completo. Tuttavia, il messaggio spoofed, indicato in denuncia, presenta l'invito a cliccare su un link non riconducibile ad un link genuino, che riporta sempre il riferimento al dominio dell'intermediario;
- l'orientamento dei Collegi dell'Arbitro Bancario Finanziario è di ritenere che nelle ipotesi di spoofing si ravvisi la colpa grave del ricorrente se si rinvengano indici di anomalia (quali ad esempio l'invito a selezionare un link in nessun modo riferibile all'intermediario o errori ortografici/di sintassi), proprio come avvenuto nel caso di specie (cfr. Collegio di Bologna, decisione n. 3072/2023);
- per prevenire truffe, ha:

i) predisposto un ulteriore presidio che permette ai clienti di essere tempestivamente informati dell'andamento del conto, attivando, in base alle circostanze che si verificano, specifici messaggi "full screen" che il cliente visualizza ad ogni accesso al proprio conto;
ii) avviato una campagna di rafforzamento del proprio piano di comunicazione alla clientela per sollecitare l'adozione di azioni tempestive di autotutela attraverso email che risultano inviate al ricorrente nel 2022 e 2023;
iii) predisposto specifiche notifiche push, che giungono sui dispositivi mobile dei clienti stessi, sul tema di prevenzione frodi inviate anche al ricorrente sul suo cellulare;
iv) previsto apposite sezioni sul sito come anche specifici articoli di supporto ai clienti al fine di informarli sulle diverse situazioni di rischio.

- il ricorrente ha eseguito tre operazioni di bonifico per acquisto di criptovaluta Bitcoin e, tramite la procedura disponibile sulla sua applicazione, ha inviato quanto acquistato ad un indirizzo di un "wallet" che gli veniva comunicato tramite SMS dall'interlocutore;
- non si capisce perché non abbia interrotto l'operazione se l'interlocutore ha manifestato la necessità di mettere in sicurezza la liquidità, ma l'operazione si è poi rilevata una disposizione di bonifico;
- si apprende dalla denuncia che la telefonata fraudolenta è giunta da un numero (*614) non riferibile alla resistente; circostanza analoga è stata valutata dal Collegio di Torino con decisione n° 3956/2023, che ne ha desunto la colpa grave della vittima di truffa:

"(…) è verosimile – da quanto allegato dall'una e dall'altra parte e da quanto documentato in atti – che il cliente sia caduto vittima di c.d. vishing. Tuttavia occorre osservare che la telefonata -"trappola" è provenuta – per affermazione dello stesso cliente (nella denuncia agli atti) – da un numero di telefono mobile non riferibile, neppure in apparenza, alla banca resistente. Vero è che il cliente ha affermato di essere stato rassicurato sulla genuinità dell'interlocuzione telefonica da un messaggio ricevuto sulla chat di messaggistica ov'è solito riceve le comunicazioni autentiche dell'intermediario; vero è anche, tuttavia, che tale messaggio spoofed di "rassicurazione", ricevuto dal cliente nel corso della telefonata-"trappola", presenta un grave errore grammaticale, che avrebbe potuto e dovuto inficiarne l'asserita capacità "rassicurante"; al contrario, avrebbe dovuto suggerire, con l'uso dell'ordinaria diligenza, una cautela addizionale nel prestar fede alle asserzioni e alle richieste del malfattore, senza contare che il predetto messaggio spoofed, nella chat riprodotta da parte ricorrente, è seguito da messaggi autentici della banca che recano un'esplicita descrizione delle operazioni in corso di esecuzione. In ogni caso va ribadito che manovre frodatorie di questo genere, per quanto segnate da un'indubbia insidiosità, non possono condurre all'esito dannoso se non attraverso la collaborazione attiva della

vittima, chiamata a condividere le credenziali di utilizzo e i codici autorizzativi imprescindibili per il completamento delle operazioni dispositive (in termini, di recente, ABF, Coll. Torino nn. 12856/22 e 457/22). All'esito, da quanto allegato e documentato dall'una e dall'altra parte, emerge la colpa grave dell'utilizzatore del mezzo di pagamento".

- in forza del contratto sottoscritto, la banca enuncia espressamente di essere estranea ai rapporti e alle controversie relative ai beni e/o servizi acquistati;
- non appena informato dell'accaduto, la resistente ha attivato le procedure di "recall" delle somme oggetto delle operazioni di bonifico qui in discussione, ma le operazioni non hanno ottenuto riscontro positivo dalla controparte. Sul punto l'orientamento dell'ABF è costante: se il mancato recupero è dovuto alla mancanza di esplicito consenso del beneficiario ovvero la richiesta di storno viene formulata quando i fondi non sono più disponibili, l'intermediario non ne risponde perché "quando l'importo di un'operazione di pagamento viene messa a disposizione sul conto corrente del beneficiario, questi ne diviene titolare e la banca non può unilateralmente bloccare o stornare il relativo importo senza il consenso del cliente in mancanza di un provvedimento giudiziale che la autorizzi a farlo" (cfr. Collegio di Napoli, decisione n. 3912/2021).
- il ricorrente ha fatto accesso al proprio Internet Banking il 31.10.2023 alle 10:55:16, in concomitanza all'orario di disposizione delle operazioni eseguite dalle ore 11:02 alle ore 11:24;
- il ricorrente ha eseguito e autorizzato le operazioni impartite che sono state autorizzate mediante ricezione della notifica push contenente il codice autorizzativo OTP di 6 cifre nonché la push autorizzativa.

Con le repliche il ricorrente precisa:

- che il 31.10.2023 è stato contattato dall'utenza telefonica n. *614, corrispondente al numero verde della banca appartenente al gruppo della resistente, da un interlocutore che si qualificava come "operatore della resistente";
- poiché ha una carta-conto prepagata, l'Iban viene offerto proprio dalla banca del gruppo: ragion per cui è stato messo nelle condizioni di potersi fidare dell'interlocutore che lo aveva contattato e che aveva dimostrato sin da subito di essere a conoscenza di ulteriori dati sensibili;
- probabilmente per l'inadeguatezza delle protezioni informatiche utilizzate, il truffatore è riuscito a bypassare il sistema di sicurezza che non ha correttamente vigilato sulle operazioni compiute dal correntista;
- ha ricevuto l'alert della truffa in corso - presidio che permette ai clienti di essere tempestivamente informati - solo diverse ore dopo l'accesso al proprio conto;
- la resistente avrebbe dovuto nutrire sospetto già dalle "operazioni preparatorie" volte ad effettuare il raggiro e, quindi, la mancata adozione delle corrette misure di sicurezza la rende colpevole dell'inganno subito dallo stesso;

chiede di accogliere il ricorso.

Nelle controrepliche l'intermediario ribadisce quanto già rappresentato con le controdeduzioni e insiste con l'evidenziare che le operazioni sono state autorizzate direttamente dalla vittima della frode.

DIRITTO

1.- Il ricorrente dichiara di essere stato vittima di frode informatica (spoofing/smishing) in data 31.10.2023 e disconosce 3 operazioni da lui stesso effettuate in pari data. Chiede il rimborso della somma sottratta pari a € 5.008,00.

2.- Le operazioni contestate sono state effettuate sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del

Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

3.- Più precisamente, il ricorrente dichiara che in data 31.10.2023 riceveva un SMS apparentemente proveniente dalla resistente, che lo informava che alle ore 10.39 era stato fatto un accesso anomalo sulla sua carta di credito (cfr. denuncia del 31/10/2023 e integrazione del 2/11/2023).

Questo Collegio, nella riunione del 12 luglio 2024, ha deliberato quanto segue, ritenendo: "necessario acquisire ulteriori elementi ai fini della decisione, invita la parte ricorrente a produrre, entro 15 giorni dalla ricezione del presente provvedimento, copia delle schermate con l'sms civetta e il registro delle chiamate. Proroga di 90 giorni il termine per l'assunzione della decisione".

La richiesta di integrazione è stata recapitata il 15/07/2024 alla parte ricorrente, che ha fornito riscontro il 30/07/2024 (entro il termine di 15 giorni assegnato dal Collegio).

Con la predetta comunicazione la parte ricorrente ha inoltrato la schermata contenente anche il messaggio truffaldino rispetto al quale può rilevarsi quanto segue: il mittente reca la denominazione della resistente; contiene errori grammaticali e di forma (passaggio dalla terza alla seconda persona singolare); il link allegato reca riferimenti all'intermediario; è preceduto da sms genuini.

4.- Nell'ambito della classica distinzione tra metodi tradizionali di frode e subdoli meccanismi di aggressione, il Collegio di Roma – richiamando un punto della motivazione della pronuncia del Collegio di Coordinamento n. 22745/2019 – ha ricondotto alla categoria delle frodi sofisticate le intrusioni truffaldine tramite "sms spoofed".

Si tratta di ipotesi di smishing in cui il messaggio 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).

Nei casi di spoofing i Collegi territoriali ABF hanno in generale evidenziato l'insidiosità del meccanismo di aggressione, consistente nell'invio dell'sms dall'utenza dell'intermediario, tale da rivelare criticità organizzative del servizio di pagamento offerto.

Tuttavia, hanno parimenti osservato che talvolta il testo del messaggio civetta presenta indici di evidente inattendibilità (quali ad esempio errori grammaticali o sintattici) o di anomalia (quali ad esempio l'invito a selezionare un link in nessun modo riferibile all'intermediario) che dovrebbero far allertare l'utente avveduto.

Si ritiene quindi che nelle fattispecie di spoofing non sia generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione, a meno che non si rinvengano i suddetti indici di inattendibilità o anomalia del messaggio. In tale ultimo caso, secondo l'ABF si può configurare un concorso di colpa tra le parti, in relazione, da un lato, alla negligenza grave del cliente che agevola il compimento della truffa e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario (Collegio di Roma, decisione n. 705/23).

5.- Le operazioni contestate sono 3 bonifici in uscita, rispettivamente di € 517,00, € 3.992,00 e € 499,00 per un totale di € 5.008,00.

Le tre operazioni sono state eseguite personalmente dal ricorrente, sotto dettatura del frodatore.

L'intermediario produce i dati relativi all'accesso all'internet banking in data 31/10/2023 (primo accesso ore 10:55) e i relativi log, da cui si evince l'impiegato dei seguenti fattori di autenticazione: utilizzo del device certificato (elemento di possesso, cfr. colonna DeviceId); fattore biometrico (elemento di inerenza).

Risulta che l'accesso sia stato effettuato proprio dal ricorrente, in quanto nei log sopra riportati compare il DeviceId associato ab origine (18/5/2022) al profilo del ricorrente.
L'intermediario produce altresì i log relativi alle tre operazioni controverse.
Da essi si ricava che l'autenticazione è avvenuta mediante l'inserimento di codici OTP, trasmessi sul device certificato con notifiche push rispettivamente alle ore 11:02, 11:16 e 11:24.
6.- A fronte di operazioni effettuate in prima persona dal ricorrente, occorre escludere l'applicabilità degli artt. 10 ss d.lgs. n. 11/2010 in tema di utilizzi fraudolenti. Infatti, l'esecuzione materiale delle transazioni da parte del cliente non consente di qualificare le stesse come "operazioni non autorizzate" ai sensi della normativa sopra richiamata.
Tale rilievo, tuttavia, non esclude che la condotta dell'intermediario possa essere comunque scrutinata in base alle regole generali del diritto delle obbligazioni, sotto il profilo del corretto adempimento delle obbligazioni contrattuali, eventualmente integrate dal principio di buona fede (Collegio di Napoli, decisione n. 6488/23, Collegio di Milano, decisione n. 8435/23, Collegio di Torino n. 15116/2022), potendosi dunque fondare la decisione sugli artt. 1375, 1176, comma 2, e 1218 c.c. (Collegio di Roma, decisione n. 2531/24).
In sostanza, sussistono elementi che possono essere presi in considerazione sotto il profilo del diligente adempimento alle obbligazioni contrattuali da parte del prestatore di servizi di pagamento (art. 1218 c.c.) e, quindi, di un concorso di colpa ex art. 1227 c.c.
7.- Con specifico riguardo al caso in esame, le tre operazioni controverse, eseguite a distanza di pochi minuti l'una dall'altra, hanno portato quasi interamente all'azzeramento del saldo della carta.
Pertanto, il Collegio accoglie parzialmente il ricorso e ritiene che la quota di responsabilità da addebitare all'intermediario in relazione alla fattispecie concreta vada determinata ex art. 1226 c.c. nella misura di euro 2.500,00 che dovrà essere versata alla parte ricorrente.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 2.500,00, 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