COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore COSIMO DAMIANO FABIO MASTROROSA

Seduta del 28/03/2025

FATTO

Parte ricorrente ha adito questo Arbitro al fine di richiedere la condanna dell'intermediario alla restituzione della somma di euro 24.100,00, corrispondente a tre operazioni di bonifico eseguite il 13, il 14 e il 15 settembre 2023 a seguito di una assunta truffa di tipo SMS spoofing e vishing dichiarando quanto di seguito.

Tra il 6 e il 14 settembre 2023 la ricorrente è stata contattata più volte, sia via SMS che per telefono, da un sedicente operatore dell'intermediario, tramite il numero verde della banca. Teoricamente i contatti erano volti a risolvere una serie di problematiche sul proprio conto corrente. Solo successivamente la parte ricorrente si è avveduta di una serie di operazioni a valere sul conto corrente intestato, per un importo complessivo di 24.100,00 euro. La ricorrente quindi ha comunicato l'accaduto all'intermediario e presentato querela il 18/09/2023. Tanto premesso, la ricorrente chiede la retrocessione dell'importo relativo alle operazioni contestate.

Nelle controdeduzioni, l'intermediario resistente rileva per quanto concerne l'autorizzazione delle operazioni:

- il 06/09/2023 il truffatore ha attivato un nuovo *mobile token* su un dispositivo diverso da quello del ricorrente, tramite le credenziali di *home banking* (elemento di conoscenza) e la digitazione del codice OTP trasmesso via SMS al ricorrente (elemento di possesso);
- l'11/09/2023 il truffatore ha effettuato l'accesso tramite il *mobile token* configurato qualche giorno prima, digitando il PIN (elemento di conoscenza) nell'app (elemento di possesso);
- ha quindi inserito un bonifico da 22.000,00 euro, autenticato sempre tramite la digitazione del PIN (elemento di conoscenza) all'interno dell'*app token* (elemento di possesso);
- con le stesse modalità, ha poi eseguito bonifici da 19.500,00 euro il 13/09/2023, da 4.000,00 euro il 14/09/2023 e da 660,00 euro il 15/09/2023.

Il bonifico da 22.000,00 euro effettuato l'11/09/2023 è stato stornato il 13/09/2023 e non costituisce oggetto della domanda. Evidenzia quindi che parte ricorrente chiede quindi il rimborso degli altri tre bonifici disconosciuti, per un totale di 24.100,00 euro. Quanto alla colpa grave, la ricorrente ha assecondato colpevolmente le richieste del truffatore, nell'ambito di una frode per nulla sofisticata. Peraltro, il messaggio civetta ricevuto conteneva un link non riconducibile all'intermediario resistente. In corrispondenza dell'attivazione del nuovo *mobile token* e delle operazioni disconosciute l'intermediario ha trasmesso appositi *alert*, di cui la parte ricorrente non ha tenuto conto.

In sede di repliche la parte ricorrente sostiene di non avere mai rivelato le proprie credenziali al truffatore e ipotizza che le informazioni devono essere state ottenute dal truffatore tramite l'accesso ai sistemi informatici dell'intermediario. Inoltre afferma che il truffatore ha sfruttato la disposizione e il successivo storno del bonifico da 22.000,00€, verificatosi realmente, per avvalorare la propria ricostruzione e accrescere la propria credibilità. Anche per le successive disposizioni fraudolente il ricorrente ha ricevuto dei messaggi di storno, che tuttavia in questo caso erano predisposti dal truffatore, ma sono stati ritenuti veritieri. In ogni caso, secondo la parte ricorrente, l'intermediario avrebbe dovuto bloccare preventivamente le operazioni in quanto anomale, dato che erano di elevato ammontare e provenivano da un dispositivo diverso da quello del ricorrente.

In ambito di controrepliche, oltre a ribadire quanto già allegato, la parte resistente esclude che il truffatore abbia ottenuto le credenziali di accesso del ricorrente tramite un'intrusione nei sistemi dell'intermediario.

La parte ricorrente chiede la restituzione della somma fraudolenta sottratta per responsabilità esclusiva dell'istituto bancario. L'intermediario chiede di voler respingere il ricorso in quanto infondato in merito.

DIRITTO

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 al 25 luglio 2023, data di entrata in vigore del Regolamento delegato (UE) 2022/2360.

In base alla denuncia in atti, il 06/09/2023 la ricorrente ha ricevuto un SMS apparentemente proveniente dall'intermediario, in cui si prospettava l'accesso al suo conto, cointestato con il marito, e si chiedeva di seguire il link allegato. La ricorrente, persuasa, ha dato seguito alla richiesta. La ricorrente riporta di essere stata, quindi, contattata telefonicamente dal truffatore, apparentemente tramite il numero verde dell'intermediario. Il sedicente operatore chiedeva di non utilizzare l'applicazione dell'intermediario per alcuni giorni e dava appuntamento telefonico a distanza di una settimana. In base ai log agli atti, il 06/09/2023 è stato configurato un nuovo *mobile token* su uno smartphone diverso da quello del ricorrente. L'11/09/2023 il truffatore ha richiamato la parte ricorrente, facendo notare che era stato disposto un bonifico da 22.000,00 € da terzi non autorizzati, ma che era stato stornato. Ha, quindi, chiesto alla ricorrente di continuare a non accedere all'app. Il bonifico è stato effettivamente riaccreditato il 13/09/2023. Con successivi contatti telefonici nei giorni seguenti, il truffatore ha continuato a chiedere alla ricorrente di non accedere all'app, affermando che erano in corso operazioni fraudolente, ma che lui si stava occupando di stornarle. Intanto la ricorrente riceve, in coda ai messaggi di *alert* relativi alle disposizioni fraudolente, dei successivi messaggi truffaldini in cui si affermava che gli importi erano stati stornati. Tuttavia, diversamente con quanto accaduto con il bonifico da 22.000,00 € dell'11/09/2023, lo storno non era veritiero. La parte ricorrente allega la denuncia fatta in data 18/09/2023.

In data 11/09/2023 risulta un SMS *alert* relativo a una disposizione di bonifico, seguito da un messaggio truffaldino in cui si riferisce lo storno e si chiede di non accedere all'app. Lo storno, tuttavia, è stato effettivamente ottenuto e risulta dall'estratto conto dei ricorrenti. È possibile che il truffatore abbia annullato il bonifico da 22.000,00 € appena disposto, per convincere la parte ricorrente a ignorare i messaggi che sarebbero stati inviati in corrispondenza ai successivi addebiti. La ricorrente afferma che l'effettivo storno del bonifico da 22.000,00 euro, avvenuto il 13/09/2023, ha contribuito a consolidare la propria fiducia e a rendere la frode sofisticata, escludendo la sua colpa grave. Tuttavia, occorre notare che, in base ai log, il truffatore era entrato in possesso delle credenziali della ricorrente e aveva configurato l'app bancaria sul proprio smartphone già il 06/09/2023. Dunque, la frode si era già perpetrata a prescindere dall'artificio costituito dallo storno del bonifico.

La prima fase della frode pare ascrivibile all'ipotesi di *smishing* con *sms spoofed*, in cui il messaggio civetta si mescola alle comunicazioni genuine correntemente trasmesse dall'intermediario. Il Collegio di Roma, con la decisione n.3750 del 16/02/2021, ha chiarito che «*ciò è possibile in quanto, attraverso l'utilizzo di appositi software in grado di modificare l'ID del mittente, i frodatori possono far sì che un sms appaia con il nome dell'intermediario. In sostanza, il messaggio truffaldino viene visualizzato sullo smartphone insieme a precedenti messaggi provenienti dall'intermediario, ingenerando nella vittima la convinzione della sua genuinità*».

La seconda fase della frode sembra riconducibile – almeno sulla base delle allegazioni di parte ricorrente – al modello del *vishing* effettuato tramite caller id spoofing, volto a simulare la provenienza della chiamata da un numero verde.

Secondo l'orientamento condiviso dei Collegi, nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, a meno che non si rinvengano indici di 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) del messaggio civetta.

Le operazioni contestate sono n. 3 bonifici effettuati a valere sul conto cointestato dei ricorrenti:

- da 19.500,00 euro il 13/09/2023;
- da 4.000,00 euro il 14/09/2023;
- da 660,00 euro il 15/09/2023.

L'11/09/2023 è stato disposto un bonifico da 22.000,00 euro, che risulta stornato con riaccredito sul conto il 13/09/2023. Questa operazione non è parte della domanda.

La parte ricorrente lamenta che l'intermediario non abbia bloccato preventivamente le operazioni di pagamento contestate, a fronte della loro natura anomala rispetto al proprio profilo di spesa.

Sul tema del monitoraggio preventivo delle operazioni di pagamento si osserva che l'art. 2 del Regolamento Delegato (UE) n. 2018/389 della Commissione prevede che gli intermediari predispongano meccanismi di monitoraggio in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente. Peraltro, in base all'interpretazione fornita dall'EBA, non è necessario che questi meccanismi operino in tempo reale – vagliando le operazioni prima della loro esecuzione –, potendo limitarsi a un monitoraggio delle frodi ex post (cfr. *ex plurimis* Collegio di Roma, decisione n. 2534 del 10/02/2022, decisione n. 707/2022, decisione n. 180/2022).

Il Collegio di Roma ha talvolta rinvenuto un obbligo di blocco di operazioni di pagamento laddove fossero integrati gli indici di frode previsti dall'art. 8, D.M. 30 aprile 2007, n. 112, che non parrebbero configurabili nel caso di specie.

Cionondimeno, codesto Collegio, con la decisione n.8019 del 28/07/2023, ha affermato che «*anche a prescindere dall'applicabilità degli indici antifrode di cui al D.M.112/2007, se le operazioni di pagamento e di prelievo per frequenza oltre che per consistenza appaiano ictu oculi assolutamente non in linea con un'operatività fisiologica, esse siano da considerare "anomale". Pertanto, l'intermediario che non abbia predisposto idonei strumenti per evidenziare e/o bloccare automaticamente comportamenti che siano evidentemente anomali, ne è responsabile*».

Secondo la ricostruzione dell'intermediario, il 06/09/2023 il truffatore ha configurato sul proprio smartphone un nuovo *mobile token*, tramite le credenziali di *home banking* (elemento di conoscenza) e la digitazione del codice OTP trasmesso via SMS al ricorrente (elemento di possesso). A conferma di questa ricostruzione l'intermediario produce il log da cui risulta l'impiego di entrambi i fattori di autenticazione. Produce, altresì, il log relativo all'invio di OTP tramite SMS al ricorrente.

Una volta configurata l'app sul proprio dispositivo, il truffatore ha potuto disporre in autonomia le operazioni, autenticandole tramite la digitazione del PIN (elemento di conoscenza) all'interno dell'app token (elemento di possesso), come sembra risultare dai log prodotti.

A seguito di ogni operazione disconosciuta risulta l'invio di SMS *alert*, che tuttavia i ricorrenti hanno ignorato perché questi *alert* venivano seguiti da SMS *spoofed* che annunciavano il presunto storno delle operazioni.

Seguendo quindi il solco interpretativo di questo Arbitro così come già citato, si ritiene configurabile la responsabilità dell'Intermediario considerato che avrebbe dovuto avvedersi dell'anomalia nelle operazioni come predisposte, anche predisponendo sistemi automatici di rilievo e/o di blocco delle operazioni (Cfr Collegio di Roma, decisione 8019 del 28/07/2023.

PER QUESTI MOTIVI

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 24.100,00.

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