

COLLEGIO DI ROMA

composto dai signori:

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

Relatore FABRIZIO MAIMERI

Seduta del 20/03/2026

FATTO

Con ricorso del 6.8.2025, parte attrice rappresenta che il 17.7.2025, alle ore 15:30, riceveva una telefonata sul cellulare: l'interlocutore, un sedicente addetto alla sicurezza della banca, lo informava di alcuni bonifici in uscita dal conto, gli suggeriva di mettere in salvo il saldo del conto corrente, ed egli seguiva le sue indicazioni fornendo il codice cliente e i tre numeri del codice di sicurezza; poco dopo, veniva messo in attesa e riceveva una notifica sulla *app* che segnalava un pagamento con PagoPA dell'importo di € 5.072,00; contattando la filiale si avvedeva di essere stato vittima di una truffa.

In sede di controdeduzioni, l'intermediario eccepisce che nella giornata del 17.7.2025, a mezzo del servizio *internet banking*, l'utente autorizzava un'operazione di pagamento per l'importo complessivo di € 5.073,30; i sistemi informatici hanno correttamente performato, contabilizzando e registrato l'operazione, regolarmente autorizzata dall'utente. La banca afferma di essere estranea alla causazione degli eventi determinanti il danno lamentato da parte ricorrente, dato che il pagamento contestato è stato eseguito tramite sistema di autenticazione e due fattori e non presentava indici di anomalia; l'evento si è perfezionato grazie alla collaborazione attiva di controparte, la quale ha indebitamente comunicato a soggetti terzi le credenziali di accesso al servizio *internet banking*, in violazione dei doveri di custodia delle credenziali ex art. 7 d.lgs. n. 11/2010. Ad ogni modo, come precisato in denuncia, controparte dichiara di essere stato contattato alle ore 15:30 del 17.7.2025, tuttavia, come appurato dai *log*, le operazioni sono avvenute in un momento antecedente (circa 20 minuti prima). Il registro telefonate prodotto da controparte non reca in alcun modo la giornata interessata ed è proveniente da casella *Outlook* di un terzo soggetto; controparte in sede di reclamo è stata invitata a segnalare l'evento all'ente beneficiario onde ottenere la restituzione del pagamento,

vista la natura indebita. Diversamente dai casi di bonifici a favore di conti correnti 'di comodo', infatti, le somme sono state percepite da un ente realmente esistente e pertanto contabilizzate all'interno del suo servizio di tesoreria (la resistente, in ottica collaborativa, fornisce il modulo per presentare richiesta di rimborso al comune beneficiario del pagamento in esame).

In sede di repliche, parte ricorrente rileva che la telefonata ricevuta era riferibile ad una utenza ufficiale della banca; il truffatore conosceva dati personali e quindi quanto accaduto è imputabile a falle nel sistema di sicurezza della banca; ha comunicato a soggetti terzi le credenziali di accesso al servizio *internet banking* in quanto ingannato dal numero e dalla conoscenza da parte del presunto operatore bancario di suoi dati personali; dallo *screenshot* allegato con le repliche appare chiaramente che il numero da cui è stato contattato era quello della banca.

In sede di controrepliche, l'intermediario osserva che il documento di cui alle repliche è difforme per *layout* ed orari a quello presentato in sede di ricorso; conseguentemente, è logico pensare come il registro chiamate prodotto non sia riconducibile a controparte (come già specificato anche in sede di controdeduzioni, in quanto contenuto in *e-mail* proveniente da terzo soggetto), ovvero che la telefonata sia avvenuta su diverso numero, ma non collegato ai rapporti bancari.

In relazione alle rispettive argomentazioni, il ricorrente chiede all'Arbitro «la restituzione dell'importo di € 5.072,00». Dal canto suo, l'intermediario chiede al Collegio: - nel merito, di rigettare il ricorso, in quanto infondato; - in via subordinata, di determinare – in caso fossero ravvisati gli estremi di un concorso di responsabilità tra le parti ex art. 1227 c.c. – l'entità delle somme; - in via di estremo subordine, di tenere in considerazione che controparte dovrà, comunque, sopportare la perdita nella misura di € 50,00, stabilita dall'art. 12, comma 3, del d.lgs. n. 11/2010.

DIRITTO

Il ricorrente chiede il rimborso di un'operazione di pagoPA eseguita il 17.7.2025 dell'importo di € 5.072,00. L'intermediario rappresenta che l'operazione è stata eseguita senza anomalie dal *device* certificato del ricorrente registrato in data 19.1.2023. L'intermediario fornisce evidenza che tutti i passaggi che hanno consentito l'esecuzione del pagamento erano presidiati da SCA. In particolare:

a) in data 17.7.2025, alle ore 15:06, il ricorrente ha effettuato un accesso (*login*) al servizio *internet banking* a mezzo *app mobile* installata sul *device* certificato (fattore di possesso) utilizzando il fattore biometrico (fattore di inerenza);

b) alle ore 15:07, all'interno della sezione "Sicurezza e Impostazioni" – disponibile sull'*app mobile*, è stato visualizzato il codice di sicurezza (*Print Mastercode*); tale codice è composto da 20 cifre, è segreto e visualizzabile dall'utente solo previa applicazione della SCA (nella fattispecie, è stata utilizzata la biometria); Nella pratica, esso è da considerarsi una sorta di codice "PUK", qualora l'utente abbia dimenticato la *password* di accesso al servizio di *internet banking*. Di tale evento, parte ricorrente è stato informato a mezzo *push in app*;

c) tale passaggio si è reso necessario poiché, contestualmente, il truffatore era collegato da *browser/PC* e aveva chiesto di recuperare la *password*. Una volta selezionata la funzione "Ho il codice di sicurezza" nella sezione di cui alla lettera precedente, il truffatore si è ritrovato di fronte una schermata che consentiva tale recupero, attraverso codici a lui noti. Infatti, una volta carpite le credenziali: 1) codice utente/alias e 2) n. 5 numeri (*random*) del codice di sicurezza (doppio fattore di conoscenza), è stato trasmesso un *sms* al numero certificato di controparte contenente un codice OTP (fattore di possesso) valevole per il *reset* della *password* alle ore 15:08; il numero di telefono presente nei *log* coincide con quello indicato nella denuncia;

d) tramite canale browser/PC, alle ore 15:09, grazie ai codici di cui sopra, il truffatore ha potuto 'sbloccare' la *password* di accesso e valida per inserire – sempre tramite medesimo canale – una richiesta di *login* (da approvarsi tramite *device* certificato);

e) alle ore 15:10, il truffatore, inserite le credenziali di cui sopra, ha inoltrato una richiesta di *login* al ricorrente che è stata approvata a mezzo fattore biometrico tramite notifica *push in app* sul *device* certificato; l'evento "autorizzativo" (*login*) è descritto nella scritta *EVENTTYPE*: "*Verify Encrypted OTP*", ossia nella verifica criptata dei dati trasmessi al *device* certificato;

f) il truffatore ha inserito alle ore 15:12 la richiesta di pagamento tramite PagoPA per l'importo di € 5.072,00 (+ € 1,30 di commissioni) da inoltrare a mezzo *push in app* al *device* certificato ai fini dell'autorizzazione;

g) la richiesta è stata autorizzata dal *device* del ricorrente alle ore 15:12 a mezzo fattore biometrico. Anche in questo caso, l'evento autorizzativo è identificato dalla voce "*Verify Encrypted OTP*".

In conclusione, da quanto rappresentato dall'intermediario e confermato dai *log* prodotti, l'operatività fraudolenta si è consumata tramite il contributo parziale del ricorrente, che ha seguito per sua stessa ammissione le istruzioni del frodatore fornendo, tra gli altri (come riporta in denuncia) le credenziali dell'*home banking* e il codice di sicurezza per cambiare la *password*.

Circa le modalità della truffa, parte ricorrente afferma di aver ricevuto una telefonata da un numero riferibile alla banca il 17.7.2025. L'interlocutore, fingendosi addetto della banca, segnalava che risultavano alcuni bonifici in uscita e che era quindi necessario trasferire il saldo su un conto sicuro. Ammette di aver seguito le istruzioni del frodatore e di avergli fornito credenziali dell'*home banking* e il codice di sicurezza.

Il numero da cui è stato contattato è riferibile alla resistente.

Nel caso di specie, la frode è riconducibile alla truffa nota come *caller id spoofing* in combinazione con messaggi di "*spoofing*". Secondo il più recente orientamento dei Collegi, la chiamata proveniente da un numero apparentemente riconducibile all'intermediario (*vishing caller id spoofing*) è equiparabile all'*sms spoofing*, con la conseguenza che, in presenza sia di *vishing caller id* che di *sms spoofing*, viene ravvisato un concorso colposo delle parti, imputando all'intermediario la colpa di «non avere adottato tutti i presidi di sicurezza necessari a impedire che il truffatore potesse [contattare] la cliente con un numero riferibile all'intermediario medesimo»: così Collegio di Roma, decisione n. 8749/2024.

L'intermediario ha osservato che l'operazione disconosciuta corrisponde a un pagamento di imposte tramite PagoPA, invitando quindi parte ricorrente a chiederne il rimborso all'ente beneficiario. A eccezione analoga il Collegio di Torino non ha dato specifica rilevanza, riconoscendo un concorso di colpa delle parti al 50% sulla base dello *spoofing* rilevato: decisione n. 10062 del 25.9.2024. Dalla lettura della pronuncia (e di altre analoghe) risulta del resto che la disponibilità degli enti beneficiari a restituire le somme è sovente subordinata all'emissione di un provvedimento dell'autorità giudiziaria.

L'intermediario fornisce evidenza di aver inviato l'*sms* con le OTP nonché notifiche *push* durante l'operatività fraudolenta. Tuttavia, nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta (come nel caso di specie) ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, il servizio di *alert* non risulta rilevante, in quanto la ricezione del messaggio non potrebbe in concreto consentire di limitare il pregiudizio dell'utente.

Alla luce delle considerazioni fin qui svolte e dell'accertamento dell'esistenza dei presupposti per un concorso di colpa fra le parti, il Collegio riconosce al ricorrente il diritto a vedersi riconosciuta la somma di € 1.500,00, a titolo risarcitorio, equitativamente determinata.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 1.500,00, 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 di procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE