

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) PIRAINO	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) CLEMENTE RUIZ	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO PIRAINO

Seduta del 18/12/2025

FATTO

Il ricorrente chiede la restituzione della somma di € 11.500,00 corrispondente all'importo di un'operazione di bonifico online eseguita fraudolentemente da terzi non autorizzati a valere sul proprio conto corrente.

In particolare, il ricorrente riferisce di aver ricevuto in data 22/05/2025 alle ore 14:26 un SMS incanalato nella conversazione genuina con l'intermediario, con cui veniva avvisato di un bonifico in uscita dal suo conto e con l'invito a contattare il numero indicato ivi indicato per ottenere ulteriori informazioni. Contattato il numero, il sedicente operatore dell'intermediario lo ha invitato a collegarsi al sito dell'*home banking* tramite un link trasmesso con un ulteriore SMS. Durante la chiamata, durata diverse ore, il ricorrente dichiara di aver ricevuto ripetuti SMS che si incanalavano in coda ad altri messaggi genuini della banca e, convinto quindi di essere effettivamente in contatto con la banca, cliccava sul link e inseriva i codici di accesso sul sito che presentava la medesima interfaccia di quello dell'intermediario. Poiché la chiamata veniva chiusa bruscamente dal sedicente operatore bancario, il ricorrente si è insospettito e, contattato il proprio referente, apprendeva di essere stato vittima di una truffa e che erano stati effettuati dal suo conto corrente n. 2 bonifici, rispettivamente di € 11.500,00 (alle ore 15:57) e di € 4.600,00 (alle ore 18:59). Alle 20:34 dello stesso giorno il ricorrente, a mezzo pec, ha chiesto alla banca il blocco delle operazioni fraudolente. Tuttavia, solo il secondo bonifico veniva impedito, per tale motivo l'odierno ricorso ha ad oggetto la restituzione della sola somma corrispondente al primo bonifico, pari ad € 11.500,00. Il ricorrente lamenta altresì che, in considerazione degli importi ingenti dei

bonifici rispetto alla usuale operatività del conto, la banca avrebbe dovuto contattarlo per sincerarsi della genuinità delle operazioni.

L'intermediario chiede il rigetto del ricorso sostenendo che sussisterebbe la colpa grave del ricorrente per aver contattato un numero non riferibile all'intermediario, nonché cliccato su un link altrettanto non riferibile alla banca, fornendo incautamente i dati necessari per effettuare le operazioni. L'intermediario sostiene altresì che l'operazione di bonifico contestata dal cliente è stata effettuata previo accesso nell'area privata, tramite credenziali personali, di cui è stata data comunicazione di *alert* sia tramite l'invio di un SMS genuino che tramite una e-mail e che in ogni caso l'operazione è avvenuta mediante autenticazione a doppio fattore, come prescritto dalla normativa vigente in materia. Sul punto l'intermediario sottolinea che è lo stesso ricorrente ad affermare in sede di denuncia di aver ricevuto i codici OTP autorizzativi inviati dalla banca. Infine, circa il mancato richiamo del primo bonifico, la banca evidenzia che le somme accreditate sul conto corrente del beneficiario erano già fuoriuscite dal conto di destinazione e comunque il bonifico era già stato effettuato essendo indirizzato verso un conto corrente acceso presso il medesimo intermediario e poiché la pec di richiesta di blocco è pervenuta solo alle ore 20:34, dopo l'orario di *cut off*.

DIRITTO

I fatti oggetto di ricorso si sono svolti in vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2). In particolare, preliminare per la risoluzione della controversia risulta la verifica dell'adozione da parte del prestatore di servizi di pagamento di una *Strong Customer Authentication* (SCA) come delineata dagli artt. 97 e 98 della PSD2, dall'art. 10 *bis* dlgs. 10/2011, dalle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea e dei criteri interpretativi dell'EBA medesima. Com'è noto, la SCA deve sussistere sia nella fase di accesso allo strumento di pagamento online sia in fase di autorizzazione delle singole operazioni dispositive e, prima ancora, in fase di eventuale *enrollment* di un nuovo dispositivo.

Con riferimento alla fase di registrazione del *device*, l'intermediario evidenzia che in data 22/05/2025 alle ore 15:35:30 è stato inserito all'interno dell'App il codice utente e la password del cliente. Alle 15:35:31 è seguito l'invio di un codice OTP tramite SMS, per validare il *device*, al recapito telefonico del cliente. Il numero di telefono corrisponde a quello dichiarato dal ricorrente in denuncia. Contestualmente il ricorrente è stato informato di un accesso anomalo, sia tramite invio di un SMS che tramite e-mail. Alle 15:36:08 è stato inserito il codice OTP all'interno della pagina dedicata alla validazione del dispositivo. La registrazione del *device* è, dunque, avvenuta mediante la modalità di autenticazione forte, grazie alla digitazione del codice utente, della password e del codice di conferma temporaneo (codice OTP) inviato per SMS sull'utenza telefonica del ricorrente. Da quanto descritto, pertanto, il sistema di autorizzazione prevede l'utilizzo di doppio fattore: conoscenza, mediante inserimento del codice utente e della password; possesso, mediante inserimento del codice OTP inviato al dispositivo del cliente. È stata dunque fornita la prova della SCA dell'*enrollment* del nuovo dispositivo.

Va ora verificata la SCA con riguardo all'accesso all'*home banking*. Tale accesso è stato effettuato tramite l'inserimento del codice utente e della password alfanumerica di esclusiva conoscenza del ricorrente, alle ore 15:50:33. L'intermediario evidenzia che, nel caso di tale secondo accesso all'App, non è stato richiesto l'inserimento del codice OTP in quanto il dispositivo utilizzato era stato già oggetto di pre-autorizzazione, come rilevato nella precedente fase, tramite l'inserimento di un codice OTP. Di conseguenza il *device* era qualificato come *trusted device*, ossia come un dispositivo fidato. Tutto ciò è avvenuto nel rispetto di quanto previsto dall'art. 10 dei *Regulatory Technical Standards* (RTS) della SCA contenuti nel Regolamento delegato (UE) 2018/389 della Commissione Europea, rappresentando

una deroga consentita e non invece una violazione della normativa SCA. Di conseguenza non è stato richiesto l'inserimento di una *password* temporanea (OTP) in quanto il dispositivo utilizzato risultava già precedentemente validato. E, infatti, completata l'autenticazione forte e registrato il device come attendibile, i successivi accessi avvengono utilizzando i seguenti doppi fattori: possesso, mediante utilizzo del *device* del cliente; conoscenza, tramite l'inserimento del codice utente e della *password*. Anche in questo caso è, dunque rispettato il doppio fattore della conoscenza e del possesso con riferimento all'operazione oggetto di analisi.

Con riferimento alla fase di disposizione del bonifico contestato, l'intermediario rappresenta che, a seguito dell'accesso all'area privata appena descritto, con inserimento a sistema del codice utente e della *password*, è stato disposto un bonifico bancario di € 11.500,00 alle ore 16:11:08 tramite l'App ufficiale dell'intermediario. L'operazione è stata poi completata tramite l'inserimento della *password* OTP, inviata al *device* del cliente in data 22/05/2025, alle ore 15:57:16. L'intermediario evidenzia, in sede sia di controdeduzioni sia di controrepliche, che i codici OTP sono sempre associati ad un'azione specifica in quanto non è possibile in alcun modo associare il codice OTP allo svolgimento di un'operazione diversa da quella per cui la *password* temporanea era originariamente predisposta. Per di più, va tenuto conto delle dichiarazioni confessorie rese in sede di denuncia dal ricorrente, il quale riporta di aver ricevuto «reiterati SMS da Banca *** con cui mi si inviavano dei codici autorizzativi». Dalle evidenze in atti emerge che il sistema di autorizzazione dell'operazione di pagamento prevede l'utilizzo di doppio fattore: riutilizzo fattore di conoscenza in fase di accesso all'home banking; possesso mediante inserimento del codice OTP inviato al dispositivo del cliente. Anche con riguardo all'operazione dispositiva è rispettato il doppio fattore della conoscenza e del possesso.

Va ora esaminato il profilo dell'eventuale colpa grave del ricorrente. Quest'ultima assume infatti rilievo solo se l'intermediario fornisce la prova di autenticazione delle operazioni che – secondo l'orientamento condiviso dai Collegi – rappresenta, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente (cfr. Collegio di Coordinamento, con decisione n. 22745/2019). Dalla denuncia resa dal ricorrente emerge che, in data 22/05/2025, alle ore 14:26, egli riceveva un SMS apparentemente proveniente dalla propria banca con cui veniva avvisato della disposizione di un bonifico di € 3.250,00. In calce al messaggio era presente un numero di telefono, simile a quello utilizzato abitualmente dal cliente per contattare la propria banca, cui rivolgersi per avere ulteriori informazioni. Non riconoscendo la disposizione di pagamento, egli contattava il numero indicato. Mentre era in contatto con il finto operatore, riceveva ulteriori due SMS, sempre incanalati nella chat genuina con la banca, con cui veniva informato del nome del presunto operatore con cui era in contatto e della corretta dissociazione del proprio dispositivo. L'interlocutore informava il cliente della presenza di diversi tentativi di bonifici in uscita e invitava il cliente ad effettuare un nuovo log-in tramite un link dal truffatore appositamente trasmesso tramite SMS. Dopo essersi collegato correttamente al link indicato dal truffatore, il cliente riceveva numerosi messaggi, allegati alla denuncia, con cui veniva informato di plurimi accessi al conto con modalità diverse e con cui venivano inoltrati codici autorizzativi di pagamenti. Durante la conversazione, durata 4 ore e 46 minuti, pervenivano all'utenza certificata del cliente ulteriori quattro SMS, sempre incanalati nella chat ufficiale con l'intermediario, con cui il cliente veniva informato del tempestivo blocco di quattro bonifici emessi senza il suo consenso. Insospettito dal modo drastico con cui il truffatore chiudeva la conversazione, il cliente contattava il proprio consulente di fiducia, prendendo atto di essere stato vittima di una truffa, verificando, tramite accesso all'home banking che erano stati effettuati due bonifici ordinari in favore di un beneficiario a lui sconosciuto, di importi pari ad euro 11.500,00 ed euro 4.600,00. Gli immediati tentativi di revoca dei bonifici non sono andati a buon fine, nonostante nessuno dei due risultasse eseguito. Il cliente, così, si rivolgeva tramite PEC all'ufficio preposto al blocco delle transazioni, chiedendo l'urgente blocco delle operazioni perché effettuate senza il suo consenso. Medesima richiesta di blocco dei bonifici eseguiti fraudolentemente è stata inoltrata all'operatore dell'intermediario contattato telefonicamente al numero verde della banca. Dalla dinamica descritta in sede di denuncia sembrerebbe che il cliente sia stato

vittima di truffa mediante la tecnica di *Smishing/sms spoofing*. Il cliente, infatti, ha ricevuto un SMS civetta che si è incanalato nella conversazione ufficiale utilizzata dalla propria banca per l'invio di comunicazioni genuine. Nello specifico, il messaggio ricevuto non presenta evidenti errori grammaticali, ma, come anche evidenziato dalla parte resistente in sede di controrepliche, si riscontrano alcuni indici di inattendibilità o di anomalia dal punto di vista sintattico, come la mancata indicazione di euro (o €) prima della cifra (3.250,00), la formula "il dispositivo è stato dissociato correttamente", per di più senza lo spazio tra l'articolo determinativo e la virgola precedente, e infine il link contenuto soltanto parzialmente riconducibile all'intermediario. L'orientamento consolidato dei Collegi reputa che nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del cliente, a meno che non si rinvenivano indici di inattendibilità o anomalia del messaggio [errori grammaticali e/o lessicali, presenza di link non riferibile all'intermediario]. In questi casi si è soliti ravvisare 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. 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. Nel caso di specie, il messaggio civetta si è inserito nella chat dell'intermediario, il messaggio non presenta sgrammaticature, ma alcuni indici di anomalia sono presenti sebbene non particolarmente evidenti. Non vi sono dunque anomalie evidenti, ma va tenuto conto che l'intermediario ha inviato al cliente nel corso della conversazione telefonica con il truffatore almeno n. 7 messaggi, tutti incanalati nella medesima conversazione con l'intermediario, con cui veniva avvisato di "accessi al conto con modalità diverse", oltre alla comunicazione di codici autorizzativi di operazioni di pagamento, tutti tramite SMS c.d. parlanti, ossia caratterizzati da un contenuto che avvisa l'utente del tipo, dell'importo e del destinatario dell'operazione che sta per autorizzare. Peraltro, l'orientamento dei Collegi reputa che il ricorso a SMS parlanti esonera dall'attivazione di un sistema di alert *ex post* (cfr. Collegio di Palermo, decisione n. 4894/25; Collegio di Palermo, decisione n. 13859/2022; Collegio di Palermo, decisione n. 5893/2023, Collegio di Torino, decisione n. 1344/2023). Alla luce di tutti questi elementi di fatto, va ritenuto che sussista la colpa grave del ricorrente in via esclusiva. E tuttavia, qualora il messaggio non presenti indici di inattendibilità ma sono rinvenibili ulteriori indici di colpa grave del cliente (per esempio, l'aver consentito al truffatore il controllo da remoto del pc o, come nel nostro caso, avere trascurato gli SMS di avvertimento dell'intermediario), il Collegio dispone il rimborso del 20% della somma richiesta (cfr. Collegio di Palermo, decisione n. 495/2025). In applicazione di questo riparto di responsabilità, al cliente la somma da restituire al cliente sarebbe pari ad € 2.300,00 (pari al 20% di euro 11.500,00).

Il ricorrente, in sede di ricorso, lamenta il tardivo blocco dei bonifici da parte della banca. In particolare, egli sottolinea di aver inviato alle ore 20:34 del 22/05/2025, giorno della truffa, una prima PEC all'intermediario con cui chiedeva il blocco dei bonifici effettuati, evidenziando che l'IBAN del beneficiario apparteneva alla stessa banca. Il bonifico contestato è stato disposto alle ore 16.11 del 22/05/2025 e l'intermediario ha rilevato che, trattandosi di bonifico effettuato su un conto incardinato presso la stessa banca, lo stesso era stato eseguito immediatamente in ottemperanza a quanto indicato all'interno del foglio informativo "Servizi di Pagamento" consultabile all'interno della sezione "Trasparenza" del sito Istituzionale, oltre che nel contratto quadro sottoscritto digitalmente dal ricorrente in data 5 aprile 2019. La doglianza non può, dunque, essere accolta.

In sede di ricorso, il cliente evidenzia che a norma dell'accordo quadro (allegato al ricorso) riportato nei fogli informativi del conto, alla voce "Rischi tipici del servizio" sia esplicitamente previsto che: «Al ricorrere di un giustificato motivo connesso con la sicurezza o con il sospetto di un utilizzo fraudolento o non autorizzato dei servizi di pagamento, la Banca si riserva la facoltà di sospendere l'esecuzione di un

ordine di pagamento in qualunque momento e anche senza preventivo preavviso, informando tempestivamente il Cliente tramite e-mail o sms o telefono o altro mezzo di comunicazione, senza assumere responsabilità alcuna per tali eventuali temporanee sospensioni, anche se non preventivamente comunicate. La Banca contatta d'iniziativa il Cliente ai recapiti da lui forniti per l'eventuale sblocco dell'ordine di pagamento bloccato per i motivi sopra indicati; nel caso in cui il Cliente confermi di aver disposto tale ordine, la Banca procede allo sblocco dello stesso». Il ricorrente sostiene di non aver ricevuto alcuna chiamata da parte dell'intermediario, per confermare il bonifico in uscita. In sede di repliche lo stesso ricorrente afferma di avere ricevuto in data 23/05/2025 una telefonata dall'ufficio sicurezza della banca nella quale gli è stato riferito che la banca avrebbe contattato il ricorrente in data 22/05/2025 alle ore 16:15 (data e orario in cui la truffa era in corso), per autorizzare il bonifico. Il ricorrente però nega di avere ricevuto tale telefonata e, sul punto, l'intermediario non ha svolto alcuna considerazione né vi è alcuna evidenza della telefonata di sicurezza. Va tenuto presente, tuttavia, che il ricorrente ha ricevuto n. 7 messaggi, tutti incanalati nella medesima conversazione con l'intermediario, con cui veniva avvisato di "accessi al conto con modalità diverse" e una email, oltre alla comunicazione di codici autorizzativi di operazioni di pagamento, tutti tramite SMS c.d. parlanti. L'intermediario resistente non ha ritenuto di esercitare la propria facoltà di sospendere le operazioni nonostante i plurimi avvertimenti e ciò suffraga la conclusione di un concorso colposo dell'intermediario, ancorché in misura minoritaria rispetto alla colpa grave del ricorrente.

Infine, in sede di ricorso e di repliche, il ricorrente evidenzia l'anomalia dell'operazione con riferimento al normale utilizzo del conto. E, tuttavia, a sostegno di tale presunta anomalia il ricorrente non allega un estratto conto da cui sia possibile evincere un utilizzo dei fondi *extra ordinem*.

In continuità con il proprio orientamento (cfr. Collegio di Palermo, decisione n. 495/2025), nonostante il messaggio presenti indici di inattendibilità non così evidenti, il Collegio rileva ulteriori elementi da cui desumere la colpa grave del cliente, quali l'aver avuto volontariamente cliccato sul *link* ricevuto, inserendo le credenziali all'interno dell'interfaccia *web*, e l'aver trascurato i molteplici sms di avviso e gli sms parlanti, equivalenti a un sistema di *alert*. Alla luce di tali rilievi il Collegio accerta il concorso colposo prevalente del ricorrente e una responsabilità dell'intermediario nella misura del 20%, anche alla luce della scelta di non sospendere i pagamenti sospetti, e, pertanto, dispone il rimborso delle somme disconosciute nella misura, per l'appunto, del 20%.

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 2.300,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE