

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) D'ANGELO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MAURILIO DANGELO

Seduta del 10/12/2025

FATTO

Con ricorso del 10 settembre 2025 (preceduto da rituale reclamo, negativamente riscontrato dall'intermediario) l'istante ha rappresentato che il 24/02/2025, verso le ore 12:30, riceveva una telefonata da un numero riconducibile all'intermediario resistente. Nello specifico un soggetto, che si presentava come operatore della banca, la informava che erano in corso operazioni sospette sul proprio conto corrente e che per questo era stato bloccato.

L'operatore la invitava a generare codici token tramite l'app della banca e a comunicarli telefonicamente, rassicurandola che si trattasse di una procedura necessaria per il blocco delle operazioni sospette e del conto corrente.

Al riguardo, contattava il proprio consulente, riscontrando che il conto risultava effettivamente bloccato ed alle ore 15:00 dello stesso giorno, lo stesso soggetto la contattava nuovamente e la invitava a generare altri codici token tramite l'app della banca, fornendole tra l'altro un nuovo PIN per l'accesso all'area riservata ed indicando che era necessario accedere per sbloccare il conto.

Orbene, pur seguendo le istruzioni, non riusciva ad accedere.

Non ricevendo alcuna ulteriore comunicazione, chiamava nuovamente la propria banca e apprendeva di essere stata truffata.

Infatti, dal proprio conto erano stati effettuati due bonifici non autorizzati dell'importo di € 9.750,00 e di € 1.370,00 verso lo stesso IBAN e intestatario.

Decideva, quindi, di sporgere denuncia contro ignoti per frode informatica ove rilevava – tra l'altro - di non aver agito dolosamente o con colpa grave; nella medesima, chiariva che l'Istituto di credito non ha adottato le misure di sicurezza e di monitoraggio adeguate a contrastare scenari di truffa, considerando che lo stesso non ha in alcun modo rilevato un anomalo utilizzo del conto corrente.

Domandava, in conclusione, la restituzione di euro 11.120,00 pari ai bonifici eseguiti in assenza di autorizzazione.

Nel costituirsi con apposite controdeduzioni, l'intermediario rappresentava che sebbene i bonifici siano stati effettuati in data 24/02/2025 e il cliente risulti avere ricevuto i dovuti messaggi di *alert*, questo ha preso contatto con la banca soltanto in data 26/02/2025 per procedere al richiamo dei citati bonifici (peraltro non annullabili, in quanto istantanei).

Ha chiarito che il cliente era a conoscenza e aveva già utilizzato il servizio di bonifico istantaneo.

Nella circostanza il ricorrente ha colpevolmente contribuito alla truffa, dando seguito alle istruzioni fornite dal terzo frodatore, ricevendo sul proprio dispositivo, le richieste di autorizzazione ai bonifici in oggetto e accettando tali richieste.

Peraltro per accedere all'area riservata e per effettuare le operazioni di giroconto e di bonifico il cliente non ha ricevuto la notifica *push* ed il sistema è quindi ricorso ad accesso con la generazione di un codice di operazione temporaneo;

In concomitanza di ogni operazione, è stato generato un nuovo codice operazione temporaneo con contestuale comunicazione alla app di notifica del cambio di sistema di autenticazione, non più online tramite *Challenge/push* autorizzativa, bensì online tramite inserimento di tale codice.

Ha rilevato di aver provato l'utilizzo dei seguenti presidi di sicurezza in ordine alla fase di accesso all'area riservata da web: 1. elemento di conoscenza: codice utente e Pin; 2. elemento di possesso: Codice Operazione temporaneo generato offline e digitato dalla Cliente sul proprio smartphone in App che genera il Codice Token sempre da App.

Tale App è installata sul dispositivo di tipo mobile di esclusiva disponibilità del Cliente, sul quale è attivo il Token dal 14/06/2023 ed in cui compare una notifica di richiesta di autorizzazione ove il richiedente fornisce la conferma con inserimento di apposito codice.

L'inserimento delle disposizioni di giroconto e di bonifico è stato effettuato dal ricorrente che ha fatto accesso all'interno della pagina riservata ai bonifici della propria APP e successivamente ha autorizzato, tramite il token installato sul proprio device, le operazioni di cui si discorre.

Ha specificato che, anche se il numero dal quale proveniva la telefonata fosse stato riconducibile alla banca, non può imputarsi all'istituto la manipolazione dei dati del mittente.

Da ciò si evincerebbe che il ricorrente ha agito in modo gravemente sprovveduto e colposo, in quanto, usando l'ordinaria diligenza, avrebbe potuto accorgersi dell'inganno in corso o comunque insospettirsi nel corso del suo evolversi

Ha pertanto richiesto il rigetto del ricorso.

Nel replicare alle controdeduzioni, la parte ricorrente ha precisato che il conto risultava effettivamente bloccato e che la successiva riattivazione è avvenuta senza alcuna sua richiesta né autorizzazione, nelle stesse ore in cui venivano disposti i due bonifici fraudolenti;

Ciò esclude qualsiasi sua colpa grave e dimostra una grave carenza organizzativa della banca, che ha consentito il riavvio dell'operatività di un conto precedentemente bloccato per sospetta frode, senza alcuna verifica d'identità né contatto con il titolare. Peraltro, l'operazione di *vishing* subita è stata caratterizzata da contatto da un numero realmente associato alla banca (*caller ID spoofing*), con la conoscenza da parte del truffatore di dati personali e bancari del cliente, blocco e successiva riattivazione del conto e induzione a generare codici Token in contesto di allarme antifrode.

Ha precisato che i log prodotti dall'intermediario sono generici, privi di legenda e di dati tecnici utili.

Infatti la semplice regolarità formale della procedura di autenticazione non libera l'intermediario dall'onere di dimostrare la riconducibilità soggettiva delle operazioni e l'adeguatezza dei presidi antifrode.

Aggiungasi, poi, che la banca aveva appena bloccato il conto per sospetta frode, circostanza che avrebbe imposto un controllo rafforzato, non già una riattivazione automatica e immediata.

Proprio perché i bonifici istantanei sono irrevocabili e non soggetti a *recall*, l'intermediario è tenuto ad adottare presidi di controllo preventivo e sistemi di monitoraggio in tempo reale idonei a bloccare o verificare operazioni sospette.

Infine, gravando sull'intermediario l'onere di provare sia l'autenticazione che la corretta registrazione dell'operazione (oltre alla colpa grave o il dolo dell'utente), l'onere non sarebbe stato adeguatamente assolto attraverso la produzione di log informatici o tracciati tecnici.

Da ciò conseguirebbe una responsabilità della Banca dipendente, tra l'altro, anche da carenze organizzative

In sede di controrepliche, l'intermediario ha precisato che il blocco del conto è avvenuto in seguito al giroconto e al bonifico di € 1.350,00.

A seguito del blocco vi è stato un contatto telefonico con il cliente che ha confermato la bontà delle operazioni effettuate e ha chiesto espressamente lo sblocco del rapporto. In tale contesto, solo il bonifico di € 9.750,00 è avvenuto dopo lo sblocco, mentre il giroconto e il bonifico sono stati effettuati prima del blocco.

Ha rilevato di aver tempestivamente attuato i presidi di sicurezza, attraverso il blocco del conto corrente.

Sussisterebbe, pertanto, la colpa grave del ricorrente, che, oltre a dare seguito alle istruzioni di un terzo sconosciuto, ha confermato la regolarità delle operazioni permettendo così che venisse effettuato il secondo bonifico.

DIRITTO

L'utilizzo fraudolento per cui è controversia è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni

interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Sul punto si rammenta che, secondo la posizione consolidata dell'ABF, la disciplina sopra citata prevede un regime probatorio di favore per l'utente di strumenti e servizi di pagamento, essendo *"ispirata al principio del "rischio d'impresa", e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi"* (così Collegio di coordinamento, decisione n. 3498/2012).

In particolare, l'art. 10 del d.lgs. 11/2010 prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare:

- A. l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti.
In particolare, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo, l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente;
- B. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

Nel merito si rileva che le operazioni contestate consistono in n.1 bonifico istantaneo tramite *home banking*, eseguito in data 24/02/2025 alle ore 13:20, per l'importo di € 1.370,00 ed in n.1 bonifico istantaneo tramite *home banking*, eseguito in data 24/02/2025 alle ore 16:08, per l'importo di € 9.750,00.

Per completezza, si osserva che l'intermediario ha dato atto che le operazioni disconosciute sono state precedute da un giroconto di € 11.500,00, effettuato nella stessa data di esecuzione dei bonifici e presumibilmente atto a creare la provvista per i successivi bonifici di importo complessivo pari a 11.120,00 (ove, per principio consolidato anche dalla decisione del Collegio di Coordinamento n. 8671/2024, vige il principio di diritto per il quale *I pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario possono essere sottratti all'obbligo della SCA anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente*).

Quanto al sistema adottato dall'intermediario rispetto alla SCA (ed alla conseguente prova di autenticazione ed esecuzione delle operazioni di pagamento), la banca ha affermato che la parte ricorrente faceva accesso all'area riservata dell'*home banking* vi a web inserendo il suo codice cliente, la sua data di nascita e il pin e autorizzando tale accesso mediante *codice token*, generato in app previo inserimento del *"codice operazione temporaneo"*.

Indi, autorizzava il bonifico in esame mediante *codice token* generato secondo la medesima procedura utilizzata in sede di accesso all'*home banking*.

Ebbene, l'intermediario ha riferito che le operazioni sono state autorizzate tramite *token* attivato sul dispositivo della parte ricorrente in data 14/06/2023, quindi diverso tempo prima dell'esecuzione dei bonifici contestati.

L'intermediario ha poi riferito che al momento dell'esecuzione delle transazioni lo *status* del *token* era "*attivo*", producendo i LOG a comprova di quanto sostenuto.

Rispetto, poi, all'accesso all'area riservata dell'*home banking*, la resistente ha riferito che il cliente faceva accesso all'area riservata dell'*home banking* via web mediante corretta digitazione del suo codice cliente e della sua data di nascita; ha poi precisato di aver positivamente controllato la coerenza tra tali dati e il codice cliente alle ore 13:04:10.

A sostegno di quanto affermato, la banca ha prodotto i correlati log.

La banca ha poi riferito (anche in tale circostanza supportando le dichiarazioni con l'allegazione dei log) che alle ore 13:00:54 il cliente digitava le tre cifre del pin richieste e confermava l'operazione cliccando sul bottone "*continua*".

Ha poi precisato di aver positivamente controllato la correttezza delle tre cifre del pin alle ore 13:01:05

L'odierna resistente ha quindi specificato (e provato) di aver preparato la notifica *push* n. ***526 per autorizzare; inoltre il cliente, non ricevendo la suddetta notifica *push*, generava in app un codice *token*, previo inserimento del "*codice operazione temporaneo*" che veniva visualizzato nella schermata del PC e inserito nell'app dalla parte ricorrente, che confermava cliccando sul bottone "*Continua*".

In ordine all'esecuzione del primo bonifico, la banca ha rilevato che il cliente, dopo aver effettuato il giroconto con codice operazione e codice token generato da app, accedeva alla pagina "*bonifici*" e predisponendo l'operazione di € 1.370,00, cliccando sul bottone "*Avanti*".

L'odierna resistente ha poi riferito che, stante il positivo esito di tali verifiche, veniva mostrata al cliente la pagina di riepilogo dei dati dell'operazione, unitamente alla relativa richiesta di autorizzazione. A sostegno di quanto affermato, ha allegato in atti le schermate esemplificative dell'area riservata dell'*home banking*.

Proseguendo, la banca ha affermato che il cliente chiedeva di autorizzare l'operazione cliccando il bottone "*Avanti*", precisando di aver successivamente effettuato i controlli per stabilire le modalità di autorizzazione, di aver preparato – alle ore 13:16:03 – la notifica *push* autorizzativa n. *** 951. e di averla successivamente inviata.

La banca ha poi riferito che la notifica *push* – in attesa di autorizzazione – sarebbe scaduta alle ore 13:20:03. L'intermediario, inoltre, ha affermato che il cliente, non ricevendo la suddetta notifica *push*, generava in app un codice *token*, previo inserimento del "*codice operazione temporaneo*" che veniva visualizzato nella schermata del PC e inserito nell'app della parte ricorrente, che confermava cliccando sul bottone "*Continua*". A sostegno di quanto affermato, la resistente ha prodotto i collegati log.

Ha quindi riferito di aver controllato, processato e contabilizzato immediatamente il bonifico, precisando di aver mostrato al cliente la pagina di conferma dell'operazione, allegando i log.

Orbene, dalle evidenze appare provata la SCA, ove – riguardo all'accesso all'*home banking* - l'elemento di conoscenza è costituito dalle tre cifre del pin (oltre a codice utente e data di nascita) e l'elemento di possesso dal codice token generato in app (previo inserimento del codice operazione temporaneo).

Quanto alle singole operazioni, rispetto all'elemento di conoscenza il medesimo è provato tre cifre del pin (mutuato dall'accesso all'*home banking*). L'elemento di

possesso si evince dal codice token generato in app (previo inserimento del codice operazione temporaneo).

In tale contesto, il Collegio rileva come l'intermediario abbia allegato e documentato, producendo le relative evidenze informatiche, che l'operazione contestata è stata autenticata tramite un sistema conforme agli standard di autenticazione multifattoriale, con regolare autenticazione, registrazione ed archiviazione della medesima. Conclusivamente questo Collegio ritiene, pertanto, che sia stata raggiunta la prova dell'autenticazione forte, nonché della corretta contabilizzazione e registrazione dell'operazione contestata, di cui l'art. 10, D.Lgs. n. 11/2010.

Dalla documentazione agli atti sembra che le operazioni contestate siano scaturite da un fenomeno di *Caller ID spoofing* (*spoofing* applicato alla chiamata) e di *Sender ID Spoofing* (*spoofing* applicato ai messaggi) realizzato ai danni di parte ricorrente.

Quest'ultima, in denuncia, ha infatti dichiarato di aver ricevuto – alle ore 12:30 circa del 24/02/2025 – una telefonata da un numero fisso (02*****89) riconducibile al servizio clienti dell'intermediario e di essersi interfacciata con un sedicente operatore bancario, il quale le segnalava tentativi anomali di bonifici da bloccare il prima possibile.

Nella circostanza, ha specificato di aver eseguito le attività indicate dal malfattore tramite la sua app mobile e di aver comunicato a quest'ultima diversi codici token apparsi sul suo *device*.

Successivamente, il truffatore le indicava di non aprire l'app della banca per alcune ore e le comunicava che l'avrebbe nuovamente contattata alle ore 15:00. Al contempo, riceveva conferma dal proprio consulente dell'avvenuto blocco del conto corrente.

Ha poi precisato di essere stata nuovamente contattata dall'operatore alle ore 15:00, ripetendo le operazioni con i token e di aver ricevuto un nuovo codice PIN per accedere all'*home banking*.

Il giorno seguente, contattava la banca, scoprendo di essere vittima di truffa e della fraudolenta esecuzione di n. 2 bonifici, di valore complessivamente pari ad € 11.120,00, disposti in favore del sig. I.D.Z. durante la telefonata avuta con il malfattore. Nell'integrare la denuncia, la medesima istante chiariva che nella giornata del 24/02/2025, tra le 12:43 e le 13:12 e tra le 16:00 e 16:06, si erano susseguiti diversi messaggi da parte dell'intermediario, con cui veniva avvertito del blocco del PIN e del nuovo PIN.

Giungevano anche messaggi riguardanti l'eliminazione del dispositivo non riconosciuto, il blocco dei bonifici e il rimborso delle somme asportate.

In proposito, si osserva che l'ID del chiamante riporta un nome collegato alla resistente, sebbene il numero mittente non sia visibile. La data e l'ora di ricezione della chiamata coincidono con quella indicata in denuncia ed il numero indicato nella medesima denuncia è riconducibile all'intermediario, il quale non ha espressamente contestato la riferibilità di tale numero ai suoi contatti, limitandosi ad eccepire come non possa essere imputata alla banca la manipolazione dei dati del mittente.

Si rappresenta altresì che constano in atti gli *screenshot* degli sms ricevuti dalla parte ricorrente durante la consumazione della frode, che risultano inseriti in una chat che reca come mittente il nome dell'intermediario.

Nei casi di spoofing, secondo la posizione condivisa dai Collegi territoriali, non è generalmente ravvisabile la colpa grave di parte ricorrente a meno che non vi siano indici di inattendibilità o anomalia che possano indurre a ravvisare un concorso di colpa

tra le parti. Nel caso in esame, è indubbio che la ricorrente abbia collaborato alla realizzazione della truffa (dando seguito alle istruzioni fornite dal terzo frodatore, ricevendo sul proprio dispositivo, le richieste di autorizzazione ai bonifici in oggetto e accettando tali richieste), ma è altrettanto rilevante la sofisticatezza della manipolazione realizzata tramite una telefonata da un numero che poteva essere considerato genuino. La valutazione circa l'eventuale colpa grave deve quindi tenere conto, da un lato, della sofisticazione e attendibilità del contatto fraudolento, rafforzato dall'apparente provenienza da canali ufficiali, e, dall'altro, della collaborazione prestata dalla parte ricorrente nello svolgimento di passaggi decisivi per l'utilizzo fraudolento per cui è controversia.

In conclusione, il Collegio ritiene sussistente un concorso di colpa fra le parti, rilevante ai sensi dell'art. 1227 c.c. e da valutarsi nella misura del 50%. Sono inammissibili le domande di corresponsione degli interessi e di rifusione delle "spese", in quanto proposte per la prima volta solo in sede di repliche (cfr. ex multis, Collegio di Torino, decisione n. 11247/2024).

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.560,00.

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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE