

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 REBECA CLEMENTE RUIZ

Seduta del 18/12/2025

FATTO

Con ricorso del 19/09/2025 il ricorrente chiede all'ABF il riconoscimento del rimborso, da parte dell'intermediario resistente, della somma di € 10.190,00 corrispondente all'importo di due operazioni di pagamento disconosciute, riferendo quanto segue:

- che in data 05/03/2024 parte ricorrente riceveva sulla sua utenza un messaggio – successivamente scomparso – da parte dell'intermediario presso il quale intrattiene un conto corrente n. ***4485;
- che cliccando sul messaggio, si apriva l'app di home banking dell'intermediario;
- che insospettito, contattava il servizio clienti dell'intermediario e, come suggerito dall'operatrice, modificava i parametri di accesso all'applicazione e di approvazione di qualsiasi operazione tramite inserimento dei dati biometrici (impronta digitale);
- che nello stesso pomeriggio, alle 16:21, veniva contattato dal numero 065***096, da un soggetto che si presentava come operatore dell'intermediario, il quale domandava se avesse compiuto tutte le operazioni necessarie al fine di mettere in sicurezza il proprio conto;
- che tale soggetto, era a conoscenza sia della precedente richiesta di assistenza, sia del suo numero di cellulare;
- che dopo circa due settimane, in data 18/03/2024, alle ore 16:50, riceveva sulla sua utenza una chiamata dal numero 023***081, da un soggetto che si presentava come operatore dell'intermediario, il quale lo informava della presenza di alcune operazioni in uscita dal suo conto corrente di dubbia origine, offrendo assistenza per l'installazione di un programma di sicurezza;

- che si interrompeva quindi la conversazione e veniva contattato dallo stesso soggetto ma da un altro numero. Tale interlocuzione si interrompeva dopo un minuto e veniva ripresa subito dopo dalla precedente utenza 023***081;
- che in questa occasione, l'operatore richiedeva di prestare il consenso all'installazione del programma di sicurezza utilizzando l'impronta digitale, ripetendo più volte l'operazione;
- che durante l'installazione del programma il telefono risultava bloccato;
- che successivamente allo sblocco iniziava a nutrire dubbi circa la genuinità della chiamata e, nel controllare il registro chiamate, si accorgeva che il numero dal quale erano provenute le chiamate era scomparso dall'elenco;
- che nel corso della telefonata, riceveva una e-mail dall'intermediario, con la quale l'intermediario comunicava di aver ricevuto l'ordine di esecuzione di un bonifico a favore di terzi di importo elevato e richiedeva di chiamare il numero verde 800***639;
- che chiamava quindi il numero verde nel tentativo di ricevere spiegazioni;
- che in data 19/03/2024, contattava ripetutamente il numero verde dell'intermediario al fine di comprendere il motivo per il quale l'app di home banking dell'intermediario, installata sul suo device con utenza 335***336, era sparita e non risultava possibile installarla nuovamente al fine di avere contezza dell'accaduto e richiedere il blocco delle operazioni sospette, da fare entro 48 ore;
- che in data 20/03/2024, faceva formale richiesta del proprio estratto conto all'intermediario e per precisare che in data 18/03/2024, aveva comunicato all'intermediario i problemi sul conto senza però ricevere alcuna precisazione in merito al numero di operazioni o agli importi a debito e/o a credito;
- che l'intermediario riscontrava la nota in data 13/04/2024, allegando estratto conto;
- che dall'estratto conto, emergeva che erano state eseguite le seguenti operazioni non autorizzate:
 - 1.- addebito di euro 7.200,00 in riferimento al quale nella sezione "concetto" è riportata la frase "Bonifici L *** S****";
 - 2.- addebito di euro 2.990,00 in riferimento al quale nella sezione "concetto" è riportata la frase "Addebito per acquisto con carta in esercizi comm.5****75 Bi*t*M**e"
- che il bonifico di importo pari ad euro 7.200,00 era stato effettuato in favore di un conto corrente aperto presso lo stesso intermediario e che l'intermediario "provvedeva prontamente ad apporre un blocco all'operatività del conto corrente beneficiario del bonifico di € 7.200,00. Ciò nonostante, parte delle somme erano già state trasferite al di fuori del conto medesimo. Le somme ancora presenti sul conto corrente di accredito sono in ogni caso custodite dalla Banca e le verranno prontamente riaccreditate a seguito di ricezione di un ordine dell'autorità giudiziaria competente in tal senso";
- che con riferimento ai fatti sopra indicati, ha sporto denuncia/querela alle autorità competenti in data 12/07/2025;
- che è evidente che l'intera vicenda faccia emergere una palese perdita di dati imputabile all'intermediario, derivante all'inadeguatezza del suo sistema informatico;
- che non è ravvisabile nei suoi confronti alcun tipo di condotta dolosa o gravemente negligente;
- che, invece, è del tutto ragionevole ricondurre tale responsabilità nell'area del rischio professionale del PSP;
- che Il fatto che la telefonata provenisse dal numero dell'intermediario, così come i messaggi oltre che la conoscenza di dati ed informazioni personali di cui era a conoscenza solo l'intermediario, ha reso la frode non evitabile nonostante l'adozione di tutte le precauzioni possibili;
- che, l'intermediario, seppur a conoscenza di quanto accaduto mentre era ancora in corso la telefonata con il numero 023***081, non ha posto in essere nessun tipo di protezione o tentativo di recupero delle somme sottratte;
- che, nel caso di specie, le operazioni non sono mai state autorizzate e il rifiuto dell'intermediario di ristorare integralmente gli importi illegittimamente sottratti non è giustificabile;
- che, nel caso di specie non è in alcun modo ravvisabile una condotta fraudolenta del pagatore e la sospensione del rimborso delle somme sarebbe totalmente destituita di fondamento;

- che, incombe sul prestatore di servizi l'onere di dimostrare che l'operazione sia stata correttamente autenticata, registrata e contabilizzata e che il malfunzionamento non sia dovuto a problematiche inerenti alle procedure esecutive o ad altri inconvenienti del sistema;
 - che, al contrario, sono rinvenibili una serie di atteggiamenti gravemente colposi dell'intermediario:
 - che il servizio clienti ha suggerito di modificare i parametri di accesso;
 - che i dati e le informazioni riguardanti il ricorrente, sono stati utilizzati per sottrarre indebitamente denaro dal conto ed erano conosciuti esclusivamente dall'intermediario;
 - che il blocco delle operazioni è stato disposto dal ricorrente; parte delle somme sottratte sono state oggetto di bonifico effettuato in favore di altro conto aperto presso lo stesso intermediario;
 - che dette circostanze denotano le responsabilità dell'intermediario;
 - che sussiste responsabilità contrattuale della banca ogni volta che non ponga in essere le misure necessarie per la sicurezza della gestione del conto e che non provveda tempestivamente ad avvisare il cliente, mediante appositi strumenti di allerta, circa i pagamenti anomali per i quali è richiesta l'autorizzazione;
 - che neppure l'apparente corretta autenticazione sarebbe stata sufficiente ad escludere la responsabilità dell'intermediario.
- Con controdeduzioni il resistente ha contestato le richieste avverse e ne chiede il rigetto, eccependo quanto segue:
- in primo luogo, le operazioni disconosciute dal cliente sono state correttamente autorizzate mediante l'utilizzo delle credenziali statiche e dinamiche in possesso del cliente stesso con autenticazione forte a due fattori (Strong Customer Authentication) e registrate e contabilizzate senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti;
 - che le operazioni venivano disposte ed eseguite dall'abituale dispositivo del cliente, verosimilmente a seguito di malware che il medesimo ricorrente ha permesso entrasse nel proprio smartphone;
 - che l'intermediario adotta un sistema di autenticazione forte per l'accesso all'area riservata, per le disposizioni di bonifico e per l'esecuzione di pagamenti online, nel pieno rispetto della normativa di settore;
 - che tutti gli accessi e le operazioni nell'area riservata del Ricorrente nei giorni precedenti alla frode e il medesimo giorno sono tutti registrati da abituale dispositivo e mediante Riconoscimento Biometrico;
 - che si avvale dell'art 10 del Reg. delegato (UE) 2018/389 che autorizza i PSP a non applicare l'autenticazione forte per il cliente qualora non siano trascorsi 180 giorni dall'ultima volta che il cliente ha avuto accesso con doppio fattore, soprattutto qualora il cliente acceda dal proprio dispositivo abituale;
 - che l'ultimo accesso con autenticazione forte è del 15/02/2024, con Riconoscimento Biometrico ed OTP ricevuta sul numero di cellulare univocamente associato al conto;
 - che pochi giorni prima della frode, il 05/03/2025, è stata registrata l'attivazione della "Conferma con Token", mediante un accesso con Riconoscimento Biometrico e inserimento di codice OTP ricevuto sul numero di cellulare;
 - che tali evidenze permettono di capire che, nessuna "anomalia" è stata riscontrata dal motore antifrode della Banca, la quale non poteva assolutamente essere a conoscenza dell'intromissione di terzi nello smartphone del cliente tramite malware scaricato dal cliente stesso;
 - che proprio in data 18/03/2024, alle 17:14:23, è stato registrato accesso con Riconoscimento Biometrico; successivamente alle 17:17:56, è stata registrata la modifica dei massimali della carta di debito del ricorrente mediante accesso con Riconoscimento Biometrico e autorizzazione tramite "Conferma del Token";
 - che nei minuti successivi venivano eseguite ulteriori modifiche dei massimali con la medesima modalità;

- che alle 17:25:43 è stata registrata una generazione del CVV dinamico della carta di debito con autenticazione forte tramite Riconoscimento Biometrico e autorizzazione tramite “Conferma del Token”;
 - che a questo punto veniva eseguito il pagamento online di euro 2.990,00 con autenticazione forte a due fattori;
 - che alle 17:39:17 è stato registrato altro accesso con Riconoscimento Biometrico;
 - che alle 17:44:05 veniva eseguito un bonifico di euro 7.200,00 sempre mediante autenticazione forte;
 - che quanto sopra dimostra non solo che le operazioni sono state correttamente eseguite con due fattori ma, soprattutto, che sono state autorizzate dallo smartphone abituale del Ricorrente con il sistema più sicuro messo a disposizione dall'intermediario e, ancora, eseguite dallo stesso cliente, che, come indicato in denuncia e nell'esposizione dei fatti, le ha autorizzate con la pressione della propria impronta sullo smartphone;
 - che non aveva alcuna possibilità di accorgersi dell'intromissione di terzi nello smartphone del ricorrente né intervenire per evitare la truffa;
 - che la truffa è ascrivibile al filone dei casi di frode condotta mediante SMS spoofing nonché vishing, ma si evidenzia innanzitutto che alcune telefonate del sedicente operatore provenivano da numeri non riferibili all'intermediario e, soprattutto, si individua certamente la colpa grave del cliente per aver verosimilmente cliccato sul link ricevuto tramite SMS e aver scaricato un'app non ufficiale, la quale ha consentito al truffatore di insediarsi nello smartphone con un malware;
 - che nessuna responsabilità può essere addebitata all'intermediario in merito al malware introdotto nel cellulare del cliente a seguito di colpevole click su link malevolo e neanche per aver autorizzato con l'impronta le operazioni,
 - che come ammesso in denuncia e nell'esposizione dei fatti, il ricorrente ha “utilizzato l'impronta digitale” mentre lo smartphone risultava bloccato e che, soprattutto, nel paragrafo precedente si è dimostrato che le operazioni sono state eseguite con “accesso con impronta digitale” (Riconoscimento Biometrico - fattore inerente) e i pagamenti confermati con “autorizzazione con impronta digitale”;
 - che con tutto quanto illustrato, la Banca non avrebbe mai in alcun modo potuto impedire l'esecuzione delle operazioni sconosciute né evitare la frode in cui è caduto vittima;
 - che in considerazione della Decisione del Collegio di Palermo n.3341/2024 “tutti i superiori elementi consentono di ritenere provata la colpa grave del Ricorrente che consentì il superamento dei presidi di sicurezza predisposti dall'Intermediario: o per averli comunicati direttamente ai truffatori, o per avere previamente installato un malware (trojan, keylogger, ecc.) che consentì ai truffatori di entrare in possesso dei dati. Non ha, invece, come detto alcun rilievo il fatto che l'SMS truffaldino risultasse apparentemente proveniente dall'Intermediario”.
 - che quella occorsa al cliente non può assolutamente considerarsi una “truffa particolarmente sofisticata”, che non si sarebbe potuta concretizzare senza l'apporto e la colpevole credulità del ricorrente;
 - che mai in alcun modo avrebbe potuto impedire l'esecuzione delle operazioni contestate;
 - che emerge con tutta evidenza la colpa grave del Ricorrente, il quale, con il proprio negligente comportamento, ha permesso la realizzazione della truffa in cui è caduta vittima.
- In sede di repliche, il ricorrente ha affermato che:
- in data 05/03/2024 a seguito di ricezione di SMS proveniente dall'intermediario, il ricorrente non compiva alcuna azione e contattava immediatamente il servizio clienti dell'intermediario;
 - il servizio clienti invitava il correntista a modificare i parametri di accesso dell'applicazione e di approvazione di qualsivoglia operazione (che prima venivano autorizzate con OTP inoltrato con SMS) con un sistema definito dall'operatore più sicuro basato per entrambi (accesso e autorizzazione) tramite il solo inserimento dei dati biometrici (impronta digitale della mano destra);

- le due operazioni oggetto del presente ricorso derivano da una telefonata ricevuta dal numero 02***081 che, come da allegati, corrisponde all'utenza clienti dell'intermediario che solo per qualche minuto si è interrotta per riprendere da altra utenza e tornare all'utenza della Banca;
- durante la chiamata il telefono era bloccato e quando alle 18:40 veniva contattato dal servizio clienti dell'intermediario, nessun operatore forniva indicazioni o risposte legate al conto, così come accadeva in data 19/03/2024 nella quale il ricorrente non avendo l'applicazione della home banking chiedeva informazioni sul proprio conto;
- da allora il ricorrente non è mai più riuscito nemmeno a verificare il conto ad averne accesso anche al solo fine della sua chiusura;
- l'affermazione dell'intermediario secondo cui il ricorrente avrebbe permesso ad un malware di accedere al proprio dispositivo, e quindi deducendo una supposta colpa grave del ricorrente appare destituita di fondamento;
- nessuna colpa grave può addebitarsi in quanto: ricevuto un SMS dalla Banca su cui non ha cliccato su alcun link ha immediatamente contattato l'operatore finanziario che ha suggerito la modifica di accesso e autorizzazione; ha ricevuto chiamate dal numero ufficiale dell'intermediario e chi parlava ha dimostrato di essere a conoscenza non solo della sua utenza, dei dati del ricorrente, della recente modifica effettuata su indicazione e guida del servizio clienti; il sistema usato da terzi è risultato particolarmente insidioso;
- lo stesso intermediario mostra di non ritenersi affidabile, come dimostrato, dal continuo inoltro di mail in cui avvisa la clientela di prestare attenzione anche alle stesse telefonate o /o contatti dello stesso intermediario;
- come evidenziato dal Codesto Arbitro in numerose decisioni, l'onere della prova della supposta colpa grave dell'utente spetta alla banca, in quanto la semplice prova dell'avvenuta autenticazione non è sufficiente ad esonerare la banca da responsabilità, soprattutto se il sistema di sicurezza presenta delle vulnerabilità che, come in questo caso, sono evidenti;
- nel caso di specie, il numero apparso sul display del cliente è quello dell'intermediario e l'interlocutore era a conoscenza di diversi aspetti e/o contatti avuti dall'utente con il servizio clienti dell'intermediario il che ha ingenerato la convinzione di affidabilità nell'utente stesso, il quale comunque contattava con altra utenza la banca, senza ottenere formali indicazioni sulla vicenda e/o ulteriori informazioni;
- dalla documentazione prodotta dall'intermediario non risulta la prova di autenticazione forte (SCA); infatti, le operazioni oggetto del presente ricorso, come evidenziato nelle produzioni avversarie, sarebbero legate all'accesso all'app attraverso impronta digitale (codice 106) e approvazione dell'operazione mediante Token (132), che in realtà non prevede alcun codice ma solo "autorizzazione con impronta digitale";
- sebbene l'intermediario qualifichi l'impronta digitale come fattore di inerenza prima e come fattore di possesso dopo, in realtà si tratta di un unico elemento e difetta in ogni caso il "fattore di conoscenza" che sarebbe stato indipendente dal dispositivo;
- la normativa richiede l'uso di almeno due di tre fattori indipendenti per verificare l'identità dell'utente o l'operazione;
- deve escludersi l'autenticazione basata su un solo fattore, inclusa l'inerenza (come un'impronta digitale o il riconoscimento facciale), che non può in alcun modo ritenersi sufficiente a costituire l'autenticazione forte del cliente (SCA) richiesta dalla PSD2;
- sussistono profili di grave inadempimento da parte dell'intermediario in relazione alla debolezza dei presidi di sicurezza informatica;
- nessuna colpa tanto meno grave è ravvisabile nella condotta del ricorrente il quale, non ha cliccato sul link del primo messaggio ricevuto ma contattato immediatamente il servizio clienti che lo guidava nella modifica dei parametri di accesso dell'applicazione;

- che il sistema di sottrazione utilizzato è risultato particolarmente sofisticato e l'intermediario, nonostante contattato contestualmente dal ricorrente da altra utenza telefonica, non è stata in grado di ovviare alla situazione;

- che il bonifico di € 7.900,00 è stato disposto illegittimamente in favore di un conto corrente aperto presso lo stesso intermediario e l'intermediario, nonostante la pronta comunicazione del ricorrente, non si è attivato in alcun modo.

Nelle controrepliche, l'intermediario resistente ha contestato le deduzioni avverse e in particolar modo ha evidenziato che:

- per quanto non richiamato nelle controrepliche, rinvia integralmente alle controdeduzioni al ricorso introduttivo;

- come dimostrato dallo stesso doc. 02 allegato alle repliche, la Banca mette a disposizione dei propri clienti diversi contenuti e informative in materia di sicurezza informatica sia tramite comunicazioni e-mail che in app, nonché anche sul web;

- come già noto al Collegio, esiste una banale tecnica che permette ai truffatori di effettuare telefonate e inviare SMS facendo visualizzare al destinatario un nome e numero prescelto in luogo del vero numero del mittente;

- il bonifico e il pagamento oggetto di contestazione sono stati eseguiti dal cliente tramite il proprio abituale dispositivo e con i sistemi più sicuri messi a disposizione dalla Banca. Difatti, contestando totalmente quanto asserito dal legale del ricorrente in merito all'assenza di prova di SCA, si ribadisce che le operazioni venivano eseguite tramite accesso con Riconoscimento Biometrico (primo fattore – fattore inerenza) e “Conferma con token” (secondo fattore – fattore possesso), nel rispetto della normativa e come dettagliatamente esposto nelle controdeduzioni;

- non vi è stato nessun malfunzionamento e alcuna compromissione dei sistemi di sicurezza della Banca, né tantomeno alcun apporto causale da parte della stessa, precisando che non poteva essere a conoscenza di ciò che accadeva al di fuori dell'area riservata del cliente né della truffa in corso e, pertanto, non poteva che considerare le operazioni correttamente eseguite, né può intervenire nella volontà dei propri clienti di disporre delle proprie finanze ed eseguire bonifici;

- con tutto quanto illustrato, la Banca non avrebbe in alcun modo potuto impedire l'esecuzione delle operazioni, correttamente eseguite e autorizzate dal cliente.

Insiste, quindi, per il rigetto del ricorso.

DIRITTO

Preliminarmente si precisa come le operazioni contestate sono state poste in essere sotto il 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), entrato in vigore il 13/01/2018.

In particolare, le fonti normative di riferimento al caso specifico sono rinvenibili negli artt. 7, 8, 10, 10 bis, 12 d.lgs. 11/2010, nonché nelle disposizioni dettate dalla normativa secondaria adottata dalle autorità di vigilanza interne ed europee (Banca d'Italia, Banca Centrale Europea, Autorità Bancaria Europea). Da quanto emerge dai documenti versati in atti da entrambe le parti, l'odierna questione riguarda la contestazione delle seguenti operazioni non autorizzate:

- bonifico di importo pari ad euro 7.200,00;

- pagamento e-commerce di importo pari ad euro 2.990,00;

Rileva, ai sensi del richiamato art. 10 d.lgs. 11/2010, l'onere dell'intermediario di provare per un verso che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti e, per altro verso, l'eventuale frode, dolo o colpa grave dell'utente.

Con riferimento alla prima operazione di pagamento e-commerce l'intermediario riferisce che per effettuare una operazione di pagamento online tramite la carta di debito, sono necessari i seguenti passaggi:

- inserire nel POS virtuale delle credenziali statiche della carta (PAN; Data di scadenza; CVV dinamico);
- confermare l'operazione di pagamento mediante l'inserimento di un codice OTP ricevuto tramite SMS sul numero di cellulare univocamente associato al conto oppure tramite "Conferma con Token" attivata in precedenza;

L'intermediario precisa che il CVV dinamico è un codice a 3 cifre che, a differenza del CVV tradizionale e per maggiore sicurezza, varia la propria numerazione dopo pochi minuti dalla visualizzazione e deve essere generato – all'occorrenza – esclusivamente dall'area riservata del cliente.

Dalla documentazione depositata da parte resistente non vi è però evidenza di quanto affermato dall'intermediario, ovvero i file log che attestino l'inserimento delle credenziali statiche nonché del CVV dinamico e quello relativo alla conferma con Token.

Le uniche evidenze risulterebbero quelle relative al "Modo autenticacion" – "CLIENTE AUTENTICADO MEDIANTE SPA EN COMERCIO ELECTRONICO", il quale indicherebbe che – stante la "Legenda LOG" – l'autenticazione del cliente sia avvenuta con doppio fattore ed eseguita online.

Posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente, i Collegi territoriali hanno condiviso che in tali ipotesi il ricorso venga accolto integralmente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente.

I Collegi hanno altresì convenuto di applicare il medesimo principio ai casi di phishing conclamato in cui l'intermediario non abbia assolto all'onere probatorio in oggetto (anche per effetto della mancata produzione delle controdeduzioni), indipendentemente dalle allegazioni del ricorrente.

Ne consegue che l'importo di euro 2.990,00, relativo all'operazione di pagamento online, deve essere rimborsato integralmente al ricorrente.

Con riferimento alla seconda operazione di bonifico di importo pari ad euro 7.200,00, l'intermediario rappresenta che per la stessa sono necessari i seguenti passaggi propedeutici:

- fare accesso al conto e cliccare su "Bonifici/Giroconti";
- inserire il beneficiario;
- indicare l'importo;
- scegliere la tipologia di bonifico;
- indicare facoltativamente la causale;

Una volta compiute tali operazioni, l'operazione andrebbe confermata mediante inserimento di OTP oppure tramite token attivato sull'app dello smartphone del cliente ("Conferma con Token") l'intermediario rappresenta che l'accesso all'area riservata tramite riconoscimento biometrico è il primo fattore (fattore di conoscenza o inerenza) mentre la OTP o la "Conferma con Token" rappresenta il secondo fattore (fattore di possesso).

Circa l'accesso in app, propedeutico al compimento dell'operazione come sopra descritto, l'intermediario precisa che si avvale dell'art. 10 del Reg. delegato (UE) 2018/389 che autorizza i PSP a non applicare l'autenticazione forte del cliente qualora non siano trascorsi 180 giorni dall'ultima volta che il cliente ha avuto accesso con doppio fattore, soprattutto qualora il cliente acceda dal proprio dispositivo abituale.

Ebbene, dalla documentazione depositata in atti risulterebbe che l'operazione sia stata autenticata mediante SCA e in particolare mediante l'utilizzo del riconoscimento biometrico (fattore di inerenza) e della "Conferma con Token" (fattore di possesso). Tali evidenze si rintracciano nella colonna I (AUTH METHOD – 106) e nella colonna J (STRONG AUTH – 132).

Tuttavia, dalla documentazione prodotta dalle parti, non si hanno evidenze circa l'offerta e/o l'attivazione di sistemi di alert per le operazioni contestate. Al riguardo si ha presente che la mancata

attivazione del servizio di sms alert (o altro assimilabile, come notifica tramite app dell'intermediario oppure e-mail, con una valutazione di equivalenza da condurre caso per caso) costituisce in genere un profilo di responsabilità dell'intermediario, salvo l'esplicito rifiuto dell'utente ad avvalersene. Dunque, l'assenza di sistemi di alert relativamente alla prima operazione delle 17:27, l'importo relativo alla seconda operazione di bonifico delle ore 17:44, pari ad euro 7.200,00, va integralmente rimborsato al ricorrente.

PER QUESTI MOTIVI

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 10.190,00.

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