COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) VITERBO	Membro designato dalla Banca d'Italia
(BA) BUSSOLI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCO GIACOMO VITERBO

Seduta del 15/07/2025

FATTO

La ricorrente riferisce di aver ricevuto dalla resistente alle ore 21:28 del 9 gennaio 2025 una mail in cui le veniva comunicato che, a seguito di una recente attività sospetta, le sue credenziali di accesso all'app e all'area clienti erano state temporaneamente bloccate.
Fa presente di aver contattato immediatamente il numero verde della banca, venendo a conoscenza che effettivamente il conto corrente e la carta di debito erano state bloccate in quanto erano state riscontrate attività sospette. Soggiunge che, nel corso della telefonata, le venivano formulate alcune domande per la redazione di un questionario necessario allo sblocco delle credenziali e che, tuttavia, la procedura si interrompeva in quanto non ricordava il saldo presente sul conto. Riferisce che le veniva chiesto di inoltrare il proprio documento e un selfie al fine di sbloccare l'account, procedura necessaria a evitare frodi.
Sottolinea che la mattina seguente, prima di inviare il selfie e il documento di riconoscimento, riceveva un SMS di autorizzazione del pagamento di € 199,99 a favore di un hotel e veniva "*di lì a breve*" contattata dal numero estero della banca. Soggiunge che, nel corso della telefonata, un operatore, che era a conoscenza dei suoi dati anagrafici e del saldo presente sul conto, riferiva che l'aveva contattata con il preciso scopo di mettere in sicurezza il conto corrente ed emettere una nuova carta di debito e che, pertanto, avrebbe generato una nuova password temporanea.
Aggiunge che, al termine della telefonata, non ricevendo alcuna password temporanea che le avrebbe consentito di accedere al conto corrente, decideva di contattare nuovamente il numero verde. Precisa che, nel corso della telefonata, l'operatore della

banca le riferiva che il suo conto corrente era ancora bloccato e che, solo a seguito di una incessante richiesta di sblocco da parte sua, l'operatore decideva di collaborare inoltrando le nuove credenziali.
Rileva che, accedendo al conto, riscontrava tre operazioni, per € 2.000,00, € 1.000,00 ed € 10.000,00, con cui era stato completamento svotato il conto corrente.
Nega di aver ricevuto o fornito ai truffatori il CVV o i codici OTP.
Fa presente, inoltre, che la frode è avvenuta mentre il conto corrente e la carta di debito nonché l'account erano bloccati per sospetta attività fraudolenta.
Segnala di non aver ricevuto *alert* per le operazioni eseguite. Richiama, sul punto, la sent. n. 378/24 della Cassazione secondo cui "*l'intermediario è tenuto a provare di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento, quali ad esempio l'invio al titolare della carta di appositi sms alert di conferma di ogni singola operazione, sulla base di un principio di buona fede nell'esecuzione del contratto*".
Lamenta che la banca, pur avendo segnalato l'esistenza di un'attività sospetta, ha dato seguito a tre operazioni, una delle quali di importo (€ 10.000,00) anomalo per la sua operatività storica, nonostante il conto fosse bloccato.
Richiama sul punto la sentenza n. 16333/16 della Cassazione che ha previsto una corresponsabilità dell'istituto di credito per non aver controllato l'andamento del conto e tempestivamente attivato di conseguenza le opportune cautele idonee ad evitare l'uso indebito della carta da parte di soggetti non abilitati, che appariva palese dall'anomalia delle operazioni effettuate, sia per numero che per importo.
Fa presente, inoltre, che la resistente non ha impostato alcun limite giornaliero o mensile per pagamenti o prelievi, né le ha proposto di stabilirlo.
Lamenta, altresì, che la banca non ha eseguito una procedura di richiamo a seguito dell'immediata contestazione.
Ritiene, infine, che la banca sia incorsa in una violazione dell'art. 2050 c.c. e dell'art. 15 del D.lgs. n. 196/03 per trattamento illecito dei dati personali. Fa presente che, trattandosi di una ipotesi di responsabilità la cui configurabilità prescinde dal comportamento doloso o colposo dell'autore, quest'ultimo – in virtù di un'inversione dell'*onus probandi* – per affrancarsi dalla presunzione di responsabilità a suo carico deve dimostrare di aver adottato tutte le misure atte ad evitare il danno avvenuto.
Chiede, pertanto, il rimborso dell'importo complessivamente sottratto, pari a € 13.000,00.
Costituitosi, l'intermediario precisa che la ricorrente è titolare di un rapporto di conto corrente e di una carta di debito collegata.
L'intermediario rileva, in primo luogo, che le operazioni disconosciute sono state autorizzate correttamente mediante l'utilizzo delle credenziali statiche e dinamiche in possesso della ricorrente con autenticazione forte a due fattori (Strong Customer Authentication) e sono state registrate e contabilizzate senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la relativa esecuzione o di altri inconvenienti. Chiarisce che, per accedere all'area riservata, tramite sito web o app, è necessario procedere all'inserimento delle credenziali statiche (username e password) scelte dal cliente o in app utilizzare i dati biometrici (impronta digitale e/o riconoscimento facciale) del dispositivo usato per accedere (riconoscimento biometrico - fattore inerenza), che, però, la cliente non aveva attivato.
Rileva, altresì, che l'autenticazione forte tramite OTP via SMS è richiesta la prima volta che il cliente accede all'area riservata oppure, successivamente, qualora siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha avuto accesso al conto mediante autenticazione forte.

Segnala che, in caso di accesso senza autenticazione forte, l'accesso è limitato alle sole informazioni relative al saldo del conto e alle operazioni di pagamento contabilizzate negli ultimi 90 giorni, mentre l'esecuzione di qualsiasi azione ulteriore richiede la previa introduzione di un secondo fattore di autenticazione.
Fa presente, sul punto, di avvalersi dell'esenzione di cui all'art. 10 del Reg. delegato (UE) 2018/389.
L'intermediario puntualizza, altresì, che ai fini della disposizione dell'ordine di bonifico occorre accedere all'area riservata, selezionare il beneficiario, scegliere la tipologia di bonifico e infine confermare l'operazione mediante l'inserimento del codice OTP inviato al numero di cellulare del cliente.
Fa presente che l'accesso all'area riservata rappresenta il primo fattore (fattore di conoscenza o di inerenza, a seconda della modalità di accesso all'area riservata utilizzata dal cliente), mentre il codice OTP rappresenta il secondo fattore (fattore di possesso) ai fini dell'autenticazione forte.
L'intermediario precisa che, per effettuare l'operazione di pagamento online tramite carta di debito, è necessario inserire nel POS virtuale utilizzato per l'esecuzione dell'operazione il PAN e la data di scadenza della carta (consultabili esclusivamente all'interno dell'area riservata, non essendo stampati sulla carta fisica), il CVV dinamico – generato dopo aver fatto acceso all'area riservata con le modalità sopra descritte (elemento di conoscenza o inerenza, a seconda della modalità di accesso all'area riservata utilizzata dal cliente) e inserito una OTP ricevuta tramite SMS (elemento di possesso) –, nonché confermare l'operazione mediante inserimento della OTP ricevuta sul numero di cellulare.
Segnala che il CVV dinamico varia la propria numerazione dopo pochi minuti dalla visualizzazione. Precisa che l'inserimento del CVV dinamico rappresenta il primo fattore (fattore di conoscenza o di inerenza, che è incluso nel processo di generazione del medesimo CVV), mentre il codice OTP rappresenta il secondo fattore (fattore di possesso) ai fini del rispetto dell'autenticazione forte. Richiama alcune decisioni recenti che considerano tale sistema "SCA compliant": Collegio Roma n. 8749/2024; Collegio Torino n. 1709/2025; Collegio Roma n. 540/2025; Collegio Roma n. 2148/2025; Collegio Roma n. 1967/2025.
Fa presente che, il giorno delle operazioni contestate, il primo accesso è stato eseguito con procedura di cambio *password* con autenticazione forte mediante inserimento di *username* scelto dalla cliente all'apertura del rapporto e di OTP ricevuta dalla stessa tramite SMS sul numero di cellulare associato univocamente al suo conto corrente, nonché inserimento di due delle quattro cifre del PIN della carta di debito della cliente prese randomicamente dal sistema.
Segnala che alle ore 11:29:55 veniva generato il CVV dinamico della carta con autenticazione forte tramite accesso con *username* e *password* e inserimento di codice OTP ricevuto tramite messaggio sul numero di cellulare univocamente associato al conto. Precisa che tale messaggio era chiarissimo in merito alle finalità del codice e metteva in guardia dal condividerlo.
Soggiunge che alle ore 11:31 veniva eseguito il pagamento di € 2.000,00 tramite inserimento delle credenziali statiche della carta (PAN e data di scadenza visibili solo all'interno dell'area riservata), del CVV dinamico generato (fattore di conoscenza) e autenticazione tramite OTP (fattore di possesso) ricevuto tramite SMS sul numero di cellulare associato al conto corrente.
Rileva che alle ore 11:36:41 veniva registrata una modifica ai massimali della carta tramite accesso con username, password nonché inserimento di OTP ricevuta tramite SMS sul numero di cellulare univocamente associato al conto.

Segnala che alle ore 11:37 veniva eseguito il pagamento di € 1.000,00 tramite inserimento delle credenziali statiche della carta (PAN e data di scadenza visibili solo all'interno dell'area riservata) nonché del CVV dinamico generato (fattore di conoscenza) e autenticazione tramite OTP (fattore di possesso) ricevuto tramite SMS sul numero di cellulare associato al conto corrente.
Segnala, infine, che alle ore 11:44:06 veniva disposto ed eseguito bonifico di € 10.000,00 tramite accesso all'area riservata con username e password e inserimento di un codice OTP ricevuto tramite messaggio SMS sul numero di cellulare univocamente associato al conto e parlante. Fa presente che la cliente riceveva anche una e-mail dalla banca per "*bonifico di importo elevato*".
Precisa che le OTP riportate nell'Allegato 6 presentano orari differenti da quelli indicati negli Allegati 3, 4 e 5 poiché la registrazione è eseguita con orario UTC.
La banca sostiene che il caso in esame sarebbe riconducibile a *vishing* misto a "*sms spoofing*" e che comunque sussiste la colpa grave della ricorrente, la quale ha dato seguito a tutte le richieste del sedicente operatore fornendo tutte le OTP ricevute, nonostante anche all'interno dei messaggi si mettesse in guardia dal non condividere tali codici. Richiama la decisione n. 6465/24 del Collegio di Milano che ha ritenuto non configurabile in un caso analogo una truffa particolarmente sofisticata ed insidiosa.
Rileva, inoltre, che la cliente sostiene di aver ricevuto sul proprio numero di cellulare una telefonata da un numero apparentemente proveniente dalla banca, ma non ha fornito alcuna prova circa la riconducibilità di tale numero all'intermediario, così da ledere inevitabilmente il diritto di difesa di quest'ultimo. Evidenzia che la ricorrente ha allegato solamente un SMS palesemente fasullo, con la richiesta di chiamare un numero assolutamente non riconducibile alla banca, come riscontrabile controllando su internet.
Fa presente che, come evincibile dallo *screenshot* dell'SMS fasullo, già il giorno precedente alla truffa la ricorrente aveva telefonato o era stata contattata da un sedicente operatore, il quale aveva fatto accesso da altra città e, in quel caso, la banca era intervenuta a porre un blocco all'operatività del conto, nonostante il luogo non fosse ignoto alla cliente, che aveva già fatto accesso da tale città precedentemente.
Soggiunge che il blocco del conto è confermato anche dall'email ricevuta dalla cliente e che il giorno successivo, sempre al telefono con un finto operatore, con la colpevole collaborazione della ricorrente e con la procedura di cambio password, è stato eseguito lo sblocco dell'area riservata della cliente e sono state correttamente eseguite le operazioni oggetto del presente ricorso.
Evidenzia, inoltre, di aver messo a disposizione dei propri clienti una misura di protezione consistente nell'invio di una notifica in APP che dia loro la certezza di essere realmente contattati dalla banca e numerosi contenuti in materia di sicurezza informatica disponibili sia sul sito web che tramite e-mail.
Chiede, pertanto, di rigettare il ricorso.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di due pagamenti online – rispettivamente, per € 2.000,00 ed € 1.000,00 – e di un bonifico di € 10.000,00 per un totale di € 13.000,00.
In via preliminare, il Collegio rileva che le operazioni oggetto del ricorso sono state eseguite 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 gennaio 2018. Inoltre, le operazioni contestate dalla ricorrente sono state eseguite successivamente all'entrata in

vigore delle disposizioni in materia di "autenticazione e misure di sicurezza" (c.d. autenticazione forte), a norma del Regolamento Delegato (UE) della Commissione, del 27 novembre 2017, n. 2018/389, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri (cfr. anche il disposto dell'art. 5, d. lgs. n. 11/2010, come novellato).

La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, comma 4, d.lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento della Banca d'Italia del 5 luglio 2011.

In particolare, ai sensi dell'art. 10, d.lgs. n. 11/2010, "qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare 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". Il comma 2 del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, "l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7" (i.e., obblighi di custodia e di corretta utilizzazione dello strumento di pagamento). Nello stesso comma è, altresì, precisato che "è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

Ai sensi del successivo art. 12, comma 2 bis, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Per "autenticazione forte" si intende "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione" (art. 1, lett. q-bis, d.lgs. 11/2010). Deve, inoltre, ritenersi che gli elementi selezionati devono essere reciprocamente indipendenti, sì che la violazione di un elemento non deve compromettere gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione.

Si deve, altresì, rilevare che l'art. 10-bis, comma 1, d.lgs. 11/2010, stabilisce che "i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

Al riguardo, il Collegio di Coordinamento ha in più occasioni precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle

operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema [...]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia). La *ratio* di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coordinamento, decisioni n. 3947/2014 e, da ultimo, n. 22745/2019, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, *ex* art. 10, comma 2, d.lgs. n. 11/2010).
Tratteggiato il quadro normativo di riferimento, il Collegio rileva che, nel caso di specie, le due operazioni di pagamento online vanno distinte dalla terza operazione di bonifico.
Quanto alle prime, l'intermediario fa presente che, per accedere all'area riservata della banca, da web o da app, è necessario: a) digitare le credenziali statiche scelte dal cliente (username e password), fattore di conoscenza, oppure, per l'app, utilizzare i dati biometrici (impronta digitale e/o riconoscimento facciale) del dispositivo usato per accedere, fattore di inerenza (che afferma non essere stato attivato dalla cliente); b) inserire l'OTP inviata al numero di cellulare del cliente la prima volta che accede oppure qualora siano trascorsi più di 180 giorni dell'ultima volta che il cliente ha avuto accesso al conto mediante autenticazione forte. Inoltre, per autorizzare i pagamenti online con carta, occorre inserire le credenziali statiche della carta (PAN e data di scadenza), inserire il CVV dinamico e confermare l'operazione mediante inserimento dell'OTP inviata via sms al numero di cellulare univocamente associato al conto corrente del cliente. Il CVV dinamico varia dopo pochi minuti dalla visualizzazione ed è generabile esclusivamente nell'area riservata della banca, previo accesso all'area riservata con inserimento di username e password o con riconoscimento biometrico (elemento di conoscenza o inerenza) e inserimento di OTP inviata al numero di cellulare indicato dal cliente in sede di apertura del conto e univocamente associato allo stesso.
Ciò premesso, il Collegio osserva che, sulla base della documentazione in atti, emerge quanto segue:
- il preventivo accesso all'area riservata il giorno della frode (10 gennaio 2025), alle ore 11:26 è stato reso possibile a seguito dell'operazione di "cambio password con autenticazione forte" e, al riguardo, risultano evidenze che l'operazione di modifica della password di accesso all'area riservata ("Proceso desbloqueo/olvido Clave" nella colonna Tipo Trans) è avvenuta mediante l'inserimento dei fattori di autenticazione richiamati dall'intermediario, come confermato dalla presenza della dicitura "MA/CE DosPosPin" nella colonna "tipo de firma" e "OTP/SMS Login" nella colonna "medio de autentication"; con tale operazione di modifica password è stato eseguito lo sblocco dell'area riservata della cliente, bloccata temporaneamente dalla banca il giorno precedente in ragione di un accesso eseguito dalla città di Napoli;

- quanto all'autenticazione dei due pagamenti online, dalle evidenze in atti risulta essere stato generato un unico CVV dinamico mediante l'utilizzo di due fattori (accesso con username e password + OTP); difatti, nella schermata allegata dall'intermediario, in corrispondenza dell'azione "Consultar datos de seguridad de una tarjeta (CVV)" eseguita alle 11:29:55 del 10 gennaio 2025, risultano le diciture "Autenticación con usuario y password personales" (Inserimento di username e password) e "Autenticación mediante OTP/SMS" (Inserimento di OTP per autorizzare attività/operazione);
- dai log si evince che, per entrambi i pagamenti online disconosciuti, è stato adoperato il medesimo CVV dinamico: ciò è coerente alle circostanze che il CVV dinamico "*varia la propria numerazione dopo pochi minuti dalla visualizzazione*" e che le due operazioni contestate sono state eseguite alle 11:31 e alle 11:37, entrambe dopo pochi minuti dalla generazione del CVV (avvenuta alle 11:29);
- nelle predette schermate è presente anche il codice "000" che, secondo la legenda, indicherebbe un'operazione correttamente autorizzata, nonché la dicitura "*cliente autenticado mediante spa en comercio electronico*", tradotto in legenda come "*autenticazione cliente con doppio fattore eseguita online*";
- risultano, altresì, in atti la tracciatura dell'SMS contenente il codice OTP necessario per confermare il pagamento online di € 2.000,00 ed il testo, riportato dall'intermediario nel riscontro al reclamo e nelle controdeduzioni, dell'SMS contenente l'OTP necessario all'autenticazione del secondo pagamento online, di € 1.000,00.

Orbene, nonostante i due elementi direttamente impiegati per l'autorizzazione dei pagamenti online (CVV dinamico generato in app; e OTP SMS inviato al cellulare certificato) siano entrambi fattori di possesso, il Collegio ritiene di conformarsi al suo precedente orientamento in base al quale "la password che entra a far parte del più complesso processo di generazione del CVV dinamico" può essere considerata un "ulteriore autonomo fattore di conoscenza richiesto ai fini della sussistenza dell'autenticazione forte" (cfr. Collegio di Bari, decisioni n. 11402/2024 e 7892/2024).

Pertanto, sulla base delle evidenze documentali versate in atti, il Collegio ritiene che il sistema di pagamento predisposto dell'Intermediario e utilizzato per le due operazioni di pagamento contestate è conforme alla definizione di SCA.

Invero, sulla base dei principi elaborati dal Collegio di Coordinamento, l'accertamento della conformità della procedura di autenticazione alla definizione di SCA contenuta nel d.lgs. n. 11/2010 non è di per sé dirimente per escludere la responsabilità del cliente. In particolare, «la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente» (decisione n. 22745/19).

Nel caso di specie, la ricorrente – sebbene affermi di essere stata contattata il giorno della frode (10 gennaio 2025) dal numero estero della banca – non allega evidenza del registro chiamate. Secondo il consolidato orientamento dell'Arbitro, la mancata allegazione del messaggio civetta o della telefonata ricevuta non consente ai Collegi di accertare se risultino o meno integrati gli estremi di un legittimo affidamento dell'utente circa la genuinità dell'interlocuzione con l'intermediario (cfr. Collegio di Bari, decisione n. 7120/2024). Inoltre, sulla base della documentazione presente agli atti, codesto Arbitro ritiene che non vi siano riscontri sufficienti per configurare una truffa particolarmente sofisticata ed insidiosa (cfr. Collegio di Milano, decisione n. 6465/24).

Ininfluente è, altresì, la mancata dimostrazione da parte dell'Intermediario dell'esistenza di un servizio di SMS alert, atteso che, dalla documentazione in atti, constano le tracciature relative agli SMS trasmessi alla ricorrente contenenti gli OTP necessari a generare il CVV dinamico, ad autorizzare il primo pagamento disconosciuto e a modificare i limiti operativi della carta. In casi analoghi, questo Collegio ha evidenziato che l'invio di messaggi siffatti "rende […] ininfluente la circostanza che non sia state fornite indicazioni circa l'operatività di un sistema Sms-Alert ex post" (cfr. Collegio di Bari, decisioni n. 189/25 e 9015/24).
Riguardo, infine, alla circostanza – lamentata dalla ricorrente – della mancata esecuzione del richiamo delle operazioni disconosciute da parte dell'intermediario, il Collegio conferma il proprio consolidato orientamento secondo il quale, una volta divenuto irrevocabile l'ordine di pagamento, il rimborso dell'operazione è subordinato al consenso del beneficiario o a un provvedimento dell'Autorità giudiziaria (cfr*., ex multis*, Collegio di Bari, decisione n. 8944/23).
Il Collegio ritiene, pertanto, non meritevole di accoglimento la domanda di rimborso delle due operazioni di pagamento online contestate dalla ricorrente.
Con riguardo al bonifico contestato, il Collegio reputa dirimente la circostanza che dal Foglio informativo del conto corrente, allegato da entrambe le parti, si evincano limiti operativi pari a € 6.000,00 sia per il singolo bonifico ordinario sia per l'importo giornaliero trasferibile con tale tipologia di operazione. Il bonifico disconosciuto, di importo pari a € 10.000,00, risulta pertanto sopra tale limite, né constano in atti variazioni contrattuali successive in ordine al predetto limite. Orbene, secondo la decisione del Collegio di Coordinamento n. 16237/18, "[l]'operazione di pagamento con la quale viene superato uno dei limiti massimi contrattualmente fissati (c.d. plafond) per l'utilizzo dello strumento elettronico di pagamento, deve essere interamente restituita al cliente in quanto, se disconosciuta, difetta del suo consenso". Difatti, "In tali casi la condotta dell'intermediario concreta la violazione delle norme pattizie poste quali obblighi di protezione gravanti sui prestatori di servizi di pagamento in ragione di un'interpretazione costituzionalmente orientata del combinato disposto degli artt. 1175 e 1375 c.c. Il limite concordato tra le parti comporta infatti che il sistema predisposto dall'intermediario debba essere impostato in modo tale da non consentire operazioni che superino il plafond, nel senso che ogni operazione eccedente debba essere bloccata automaticamente (tale requisito è necessario perché il sistema si possa ritenere conforme ai presidi di sicurezza imposti dalla legge). Se ciò non avviene l'intera operazione è per ciò stesso illecita, in quanto vìola il limite di operatività della carta sul quale il cliente fa affidamento e deve ritenersi ipso facto non autorizzata se disconosciuta (ex art. 10, comma 1, D.lgs. 11/2010)."
Inoltre, dalla documentazione versata in atti, si evince che il bonifico è stato autorizzato alle 11:44 del 10 gennaio 2025 mediante accesso all'area riservata con *username* e *password* e inserimento di un codice OTP trasmesso tramite SMS, ma il Collegio rileva che non consta in atti evidenza dell'invio dell'SMS contenente l'OTP necessario all'autenticazione di tale operazione.
Pertanto, il Collegio dispone che l'intermediario rimborsi alla ricorrente l'importo del bonifico contestato.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 10.000,00.
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

Firmato digitalmente da
ANDREA TUCCI