Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI COORDINAMENTO

composto dai signori:

(CO) MAUGERI	Presidente
(CO) TINA	Membro designato dalla Banca d'Italia
(CO) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(CO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(CO) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore TENELLA SILLANI

Seduta del 27/02/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa con l'intermediario nella fase prodromica del presente ricorso, espone quanto segue. In data 10/03/2025, alle ore 9:38, riceveva un SMS, all'apparenza proveniente dall'intermediario convenuto, che la informava dell'avvenuta disposizione di un bonifico di importo pari ad € 199,00, altresì indicandole un'utenza cui rivolgersi nel caso l'operazione non fosse a lei riconducibile. Convinta della genuinità della comunicazione, contattava il numero segnalato; le rispondeva un sedicente operatore dell'ufficio frodi della banca che le chiedeva la terza lettera della *password* d'accesso all'*home banking*, al fine di procedere con il riconoscimento del suo *account* bancario. Una volta effettuato l'accesso, il sedicente operatore le rappresentava la necessità di bloccare un addebito anomalo sul suo conto corrente (di € 199,00) da parte di una società albanese, nonché un'ulteriore richiesta di addebito (di € 1.900,00) proveniente da altra società albanese. Dato l'assenso alla predisposizione del blocco delle due operazioni, nonché al blocco operativo del conto corrente, veniva aperto un nuovo conto corrente dal sedicente operatore che le comunicava credenziali ed Iban al fine di provvedere alla girata di una somma pari a € 4.225,77, che lei eseguiva come da istruzioni. Allertata dallo stesso sedicente operatore che anche su un altro c/c presso un diverso intermediario vi fossero operazioni di addebito, veniva convinta ad effettuare un bonifico di € 850,00 a

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

favore del nuovo conto corrente, quale procedura necessaria per bloccare gli assunti addebiti a lei sconosciuti. Di seguito, si avvedeva trattarsi di un pagamento *e-commerce* di pari importo, disposto con la propria carta e da lei mai autorizzato. Il falso operatore la invitava infine a disinstallare e successivamente installare l'*app* dell'*home banking* e ad attendere le credenziali relative al nuovo c/c. Non ricevendo comunicazione alcuna, contattava il Numero Verde dell'intermediario convenuto e così apprendeva di essere stata vittima di una truffa, prontamente denunciata all'Autorità competente. Tutto ciò premesso, chiede la ripetizione del controvalore dei pagamenti fraudolenti, oltre alla rifusione delle spese di assistenza difensiva.

L'intermediario, ritualmente costituitosi, precisato che la ricorrente è titolare presso di sé di un c/c e di una carta di debito; che la prima operazione disconosciuta è un bonifico emesso dal dispositivo abituale della cliente; che la seconda è un pagamento *online* effettuato mediante la carta di debito alla stessa riconducibile, sostiene che le operazioni sono state correttamente contabilizzate, registrate e autenticate, risultando poste in essere con il corretto inserimento delle credenziali e senza anomalie. Descrive, in particolare, le modalità di accesso all'area riservata e, di seguito, quelle di disposizione del bonifico e del pagamento tramite carta di debito. Evidenzia che il carattere irrevocabile dell'ordine di bonifico (come chiarito alla ricorrente dal Servizio Clienti cui la stessa si era rivolta) è conforme all'art.17 del D.lgs. n.11/2010, nonché a quanto indicato in sede di stipulazione del contratto. In considerazione degli accadimenti narrati dalla parte ricorrente, ritiene che sia stata vittima di *vishing/SMS spoofing* ed abbia tenuto un comportamento connotato da colpa grave. Sottolinea, per contro, la correttezza del proprio agire per essersi tempestivamente attivato per bloccare il conto e per tentare di recuperare le somme sottratte. Chiede, pertanto, il rigetto del ricorso.

Alle controdeduzioni replica la ricorrente la quale - confermando quanto già rappresentato in sede di ricorso - ribadisce il carattere formalmente attendibile dei messaggi rivelatisi truffaldini in quanto in apparenza riconducibili alla propria banca e, conseguentemente, l'assenza di colpa grave nel suo comportamento. Con le controrepliche l'intermediario, confermando quanto già esposto, insiste per il rigetto del ricorso, sottolineando la natura palesemente fasulla dell'SMS civetta ricevuto dalla cliente, vittima di una truffa non particolarmente sofisticata.

Il Collegio di Milano, avanti al quale è stato proposto il ricorso, "*considerate la presenza di decisioni difformi tra i vari Collegi territoriali sulla questione relativa all'applicabilità dell'art. 10 del Regolamento Delegato UE n. 2018/389, come modificato dal Regolamento Delegato UE n. 2022/2360, nonché la rilevanza della questione legata alla natura del CVV dinamico quale fattore di autenticazione*", ha sospeso il procedimento e rimesso gli atti al Collegio di Coordinamento ai fini della decisione, in conformità a quanto stabilito alla Sez. III, par. 5 delle "*Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari*" emanate dalla Banca d'Italia.

DIRITTO

La ricorrente chiede l'accertamento del proprio diritto alla restituzione del controvalore di due operazioni dalla stessa disconosciute, effettuate tra le 10:01 e le 10:25 del 10/03/2025, per il

complessivo importo di euro 5.075,77. Ai due pagamenti contestatati si applica la disciplina di cui al d.lgs. 27.01.2010, 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. PSD2 - *Payment Services Directive* 2). Come è noto, la richiamata normativa, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, prevede una serie di obblighi a carico sia dei fruitori sia dei prestatori di servizi di pagamento.
Ai primi, è imposto di usare detti strumenti in modo corretto e diligente - secondo le prescrizioni contrattuali -, di garantire la segretezza dei codici necessari per usufruire dei servizi, di informare tempestivamente i prestatori in caso di operazioni fraudolente (cfr. art. 7, comma 3 del d. lgs. n. 11/2010, secondo cui l'utente "*adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate*"). I secondi sono tenuti a predisporre adeguati sistemi di sicurezza che impediscano a terzi l'accesso ai dispositivi personali degli utilizzatori; laddove venga disconosciuta un'operazione (perché effettuata in conseguenza di furto, smarrimento, illecito utilizzo da parte di terzi degli strumenti di pagamento e dei connessi codici dispositivi) devono "*provare che 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*" (art. 10, comma 1 del d. lgs. n. 11/2010).
Con riguardo, in particolare, all'autenticazione, deve ancora richiamarsi l'art. 10 *bis*, comma 1, del d.lgs. n. 11/2010, il quale, recependo l'art. 98 della direttiva UE 2015/2399 (PDS2), sancisce l'obbligo per i prestatori di servizi di pagamento di applicare "*l'autenticazione forte del cliente*" (c.d. SCA: *strong customer authentication*) nei casi in cui questi acceda al proprio conto di pagamento *on line*, effettui un'operazione di pagamento elettronico o "*qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*". Relativamente a tutte le predette fasi, la SCA si considera realizzata quando ricorrano almeno due dei seguenti tre fattori, reciprocamente indipendenti e appartenenti a categorie diverse: conoscenza, inerenza, possesso. Gli intermediari non sono soggetti ai doveri sopra descritti solo se l'operazione contestata è stata direttamente disposta dal titolare dello strumento di pagamento, sia pure in conseguenza di una frode perpetrata da terzi.

Nel caso in esame, dalle dichiarazioni rese dalla ricorrente nella denuncia e nel ricorso sembrerebbe che i pagamenti dei quali domanda il rimborso siano stati eseguiti con il suo contributo causale solo parziale, per cui si deve escludere che possano essere considerati eseguiti personalmente dalla stessa, con conseguente applicabilità della richiamata disciplina protettiva. In proposito, è infatti orientamento consolidato dei Collegi che se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es., inserisce uno solo dei fattori di autenticazione) la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo deve essere prestato nella forma convenuta tra il pagatore e il prestatore dei servizi di pagamento. Da ciò consegue che l'intermediario convenuto è tenuto a provare di aver applicato la SCA in tutte le fasi delle contestate operazioni, secondo la disciplina dettata dal legislatore.
Con riguardo alla fase di accesso all'area riservata, dai *log informatici* versati in atti, nonché dalla legenda esplicativa risulta che - nel giorno della truffa - sono stati effettuati diversi accessi dall'applicazione presente sul dispositivo della cliente, tra i quali quello prodromico all'esecuzione delle

due operazioni disconosciute, eseguito alle ore 09:55,31, autorizzato mediante il solo inserimento di *username* e *password.* In proposito, l'intermediario ha precisato che tale accesso è avvenuto senza la necessità dell'inserimento di un secondo fattore di autenticazione, in applicazione dell'art. 10 del Regolamento Delegato (UE) 2018/389, che autorizza i PSP a non applicare la SCA qualora non siano trascorsi più di 180 giorni dall'ultima volta che il cliente ha effettuato un accesso con doppio fattore. La parte resistente ha quindi giustificato l'assenza di un secondo fattore di autenticazione dimostrando documentalmente che vi fosse stato un precedente accesso (in data 02/12/2024 alle ore 10:51:27) eseguito mediante l'impiego di entrambi i fattori di autenticazione: inserimento di *username* e *password* (fattore di conoscenza) e codice OTP (fattore di possesso), inviato via SMS al numero di telefono della ricorrente.
Come evidenziato dall'ordinanza di rimessione del Collegio di Milano, vi sono opposti orientamenti in seno dell'Arbitro circa la effettiva conformità al dato normativo della sopra descritta procedura adottata dall'intermediario resistente e cioè in ordine al campo di applicazione del regime di esenzione dalla SCA di cui all'art. 10 del Regolamento (UE) 2018/389 (come modificato dal Regolamento Delegato (UE) 2022/2360) previsto in ipotesi di accesso cd. informativo.
Secondo tale disposizione: "*I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, fatto salvo il rispetto dei requisiti di cui all'articolo 2, se l'utente dei servizi di pagamento accede direttamente al suo conto di pagamento online, a condizione che l'accesso sia limitato a uno dei seguenti elementi online senza che siano divulgati dati sensibili relativi ai pagamenti: a) il saldo di uno o più conti di pagamento designati; b) le operazioni di pagamento eseguite negli ultimi 90 giorni attraverso uno o più conti di pagamento designati. 2. In deroga al paragrafo 1, i prestatori di servizi di pagamento non sono esenti dall'applicazione dell'autenticazione forte del cliente se una delle seguenti condizioni è soddisfatta: a) l'utente del servizio di pagamento accede online alle informazioni di cui al paragrafo 1 per la prima volta; b) sono trascorsi più di 180 giorni dall'ultima volta che l'utente del servizio di pagamento ha avuto accesso online alle informazioni di cui al paragrafo 1 ed è stata applicata l'autenticazione forte del cliente*".

Con specifico riguardo al regime di esenzione dalla SCA previsto dalla sopra richiamata norma, occorre in particolare chiarire se, una volta avuto accesso al conto mediante ricorso a un unico fattore, sia o meno ammissibile il riutilizzo di detto fattore in combinazione con un secondo elemento di autenticazione per autorizzare un'operazione di pagamento.
Sulla questione si è espressa la *European Banking Authority* (EBA) offrendo due specifiche indicazioni. Con la Q&A 2018_4141, dopo aver ribadito che il regime di "*strong customer authentication*" di cui all'art. 4 del Regolamento delegato deve essere rispettato tanto nella fase di accesso al conto dell'utilizzatore, quanto nella fase di disposizione di un pagamento, ha precisato che possa essere riutilizzato uno dei fattori utilizzati al momento dell'accesso nell'ambito della medesima sessione per disporre un'operazione di pagamento, purché l'associazione di entrambi i fattori produca il *dynamic linking* (e cioè "*a condizione che l'elemento di collegamento dinamico richiesto dall'articolo 97(2) PSD2 e dettagliato dall'articolo 5 del regolamento delegato sia presente e collegato*" al pagamento stesso). A titolo di esempio è stato esaminato il caso di un iniziale accesso (con SCA) tramite nome utente e *password* (fattore di conoscenza) più OTP via SMS (fattore di possesso) in relazione al quale l'utente prima consulta gli estratti conto e poi, all'interno della medesima sessione (che termina dopo 5 minuti)

dispone un pagamento. In proposito, viene confermato che, ai fini della SCA, è sufficiente il fattore di conoscenza (già utilizzato per l'accesso) in combinazione con il fattore di possesso utilizzato per l'esecuzione dell'operazione.
Se nel 2018 l'EBA si è pronunciata solo in relazione all'ipotesi di accesso con doppio fattore e riutilizzo di uno di tali fattori per eseguire il pagamento, con la Q&A 2020_5516 affronta la stessa questione, ma con riguardo ad un accesso avvenuto con un solo fattore da riutilizzare per il compimento della successiva operazione dispositiva. Al riguardo afferma che il principio formulato con la Q&A 2018_4141 (sul riutilizzo, in fase dispositiva, del fattore di autenticazione utilizzato in fase di accesso) trova applicazione anche quando l'accesso al conto non sia presidiato da SCA, in quanto riconducibile a una delle ipotesi per le quali è prevista l'esenzione ai sensi dell'art. 10 del Regolamento delegato.
L'EBA altresì precisa che la Q&A 2018_4141 non esclude la possibilità che i prestatori di servizi di pagamento possano "*riutilizzare un elemento utilizzato per accedere ai conti di pagamento online ai sensi dell'esenzione di cui all'articolo 10 del Regolamento delegato quando avviano una transazione di pagamento elettronico a distanza nella stessa sessi*one", a condizione che siano soddisfatti i requisiti stabiliti nelle precedenti indicazioni del 2018, ossia che l'accesso e il pagamento siano avvenuti nella medesima sessione e sia garantito il *dynamic linking*.

Anche alla luce delle indicazioni offerte dall'EBA, alcuni Collegi territoriali hanno ritenuto conforme al quadro normativo di riferimento e, in particolare, al regime derogatorio di cui all'art. 10 del Regolamento delegato, la procedura posta in essere dall'intermediario che consente ai clienti, al momento dell'accesso all'area riservata preliminare alla effettuazione di un'operazione di pagamento, di riutilizzare uno solo dei fattori di autenticazione impiegati in un precedente accesso, eseguito nell'arco di 180 giorni (Coll. Roma, dec. n. 7918/2024; n. 3963/2024), "riutilizzo" che si considera ammissibile sia che l'accesso al conto sia avvenuto con una SCA completa, sia che esso sia avvenuto con esenzione da SCA qualora si tratti di accesso informativo e sempre rispettando le condizioni previste dall'art. 10 Regolamento delegato (Coll. Torino, dec. n. 9093/2024; n. 9705/2024). Di contro, altri Collegi - tra cui quello di Milano - hanno invece considerato il regime di esenzione dalla SCA, disciplinato dal richiamato art. 10, operante soltanto per gli accessi di carattere informativo di cui al comma 1 di detta disposizione, eseguiti entro 180 giorni rispetto al primo (Coll. Milano, *ex multis*, dec. n. 5970/2025; n 3619/2025; n. 93/2025; n. 10636/2024, n. 8155/2024 e n. 7574/2024; Coll. Bologna, dec. n. 11652/2024, n. 9591/2024; Coll. Bari, dec. n. 6380/2024).
Secondo il Collegio rimettente l'EBA non avrebbe inteso estendere la regola anche alle operazioni dispositive, per le quali continuerebbe quindi ad essere "*necessariamente richiesto un nuovo accesso (non più di carattere informativo, ma esclusivamente strumentale all'esecuzione del pagamento), il quale dovrebbe arrivare a godere dell'esenzione soltanto per il fatto di essere effettuato entro 180 giorni dal primo*" accesso con SCA Si sostiene, più in particolare, che l'Autorità avrebbe semplicemente chiarito che, laddove l'accesso all'area personale sia avvenuto ai sensi dell'art. 10, comma 1, del Regolamento delegato e l'utilizzatore, nella medesima sessione, intenda dar luogo ad una operazione di pagamento, questi possa beneficiare dello speciale meccanismo di autenticazione. Da ciò è fatto conseguire che "*il cliente che ha eseguito l'accesso mediante un unico fattore di autenticazione (proprio perché di carattere informativo) possa riutilizzarlo al momento del pagamento unitamente ad un secondo fattore, a cui sia riferito un collegamento dinamico ex art. 97, comma 2, della direttiva sui*

servizi di pagamento". Si afferma, d'altra parte, che se si ammettesse un'applicazione ampia del regime di esenzione si verrebbe ad introdurre "*un doppio regime di esenzione (in fase di primo accesso informativo e poi in fase di secondo accesso, prodromico al pagamento)* [un esito] *che inevitabilmente frustrerebbe la stessa* ratio *che ha ispirato l'introduzione della* strong customer satisfaction".
Oltre alle divergenti prospettive sopra richiamate, l'ordinanza di rimessione del Collegio di Milano prospetta altresì una diversa e più rigorosa interpretazione delle indicazioni offerte dall'EBA, secondo la quale - in coerenza con la *ratio* cui è informata l'intera disciplina dei servizi di pagamento - l'esenzione dalla SCA sarebbe limitata ai soli accessi di carattere informativo, occorrendo invece l'autenticazione mediante l'inserimento del doppio fattore (senza alcuna possibilità di riutilizzarne soltanto uno) ogni qualvolta l'utente intenda porre in essere un'operazione di pagamento, anche laddove ciò avvenga nell'ambito di una sessione avviata con un accesso informativo che abbia usufruito del regime di esenzione.
In relazione a quest'ultima opzione ermeneutica il Collegio di Coordinamento condivide le perplessità già evidenziate dal Collegio rimettente, dal momento che tale lettura, ancorché ispirata ad un rigoroso rispetto dei requisiti di sicurezza imposti dalla normativa *de qua*, porterebbe a travalicare i chiarimenti ufficiali dell'EBA, i quali, ancorché di natura non vincolante (trattandosi di "*soft law*"), rappresentano comunque interpretazioni autorevoli della normativa europea in materia bancaria, finalizzate ad orientare le prassi applicative all'interno degli Stati membri e, quindi, a promuovere un quadro regolatorio uniforme in materia di *governance* creditizia (così, ai sensi dell'art. 16 del Regolamento EBA (modificato con regolamento 2019/2175) secondo cui "*Le autorità e gli istituti finanziari competenti compiono ogni sforzo per conformarsi agli orientamenti e alle raccomandazioni*"). In correlazione con tali obiettivi, il principio del "*comply or explain*" (espressamente affermato per orientamenti e raccomandazioni: cfr. art. 16 *bis* e *ter* del sopra citato Regolamento) stabilisce l'obbligo di dare adeguata motivazione nel caso si intenda non conformarsi alle indicazioni fornite dall'EBA. A conferma della significativa rilevanza di tali strumenti di *soft law* può altresì richiamarsi la decisione della Corte di Giustizia del 15 luglio 2021, causa C-911/19, la quale ha stabilito che gli orientamenti dell'EBA, pur non essendo vincolanti, sono sottoponibili al controllo giurisdizionale della Corte UE, e cioè possono essere valutati ai sensi dell'art. 267 TFUE, ossia nell'ambito di un rinvio pregiudiziale).

Proprio l'importante ruolo che svolgono le indicazioni che provengono dall'EBA porta questo Collegio a ritenere non coerente con il chiaro dettato delle Q&A (del 2018 e del 2020) la tesi secondo cui il regime di esenzione dalla SCA, disciplinato dall'art. 10 del Regolamento (UE) 2018/389, operi soltanto per gli accessi di carattere informativo di cui al comma 1 di detta disposizione, eseguiti entro 180 giorni rispetto al primo, dovendosi conseguentemente procedere ad un nuovo accesso con l'utilizzo di un doppio fattore se si intenda procedere ad un'operazione di pagamento. Tale interpretazione, infatti, si discosta dalle indicazioni dell'EBA, comportandone un evidente ed immotivato superamento.

Il Collegio ritiene pertanto conforme al quadro normativo di riferimento, nonché alle correlate indicazioni interpretative offerte dall'EBA, il procedimento che consente (in applicazione del regime di esenzione di cui all'art. 10 del Regolamento Delegato (UE) 2018/389) di accedere all'area riservata utilizzando uno solo dei fattori di autenticazione impiegati in un precedente accesso avvenuto - con una SCA completa - entro l'arco temporale di 180 giorni, fattore che può essere riutilizzato per autorizzare

un'operazione di pagamento (e cioé "*quando* [si avvia] *una transazione di pagamento elettronico a distanza nella stessa sessione*": Q&A 2020_5516), purché accompagnato da un altro fattore di diversa natura per garantire il "*dynamic linking*" (così Q&A 2018_4141: "*a condizione che l'elemento di collegamento dinamico richiesto dall'art. 97 (2) PSD2 e dettagliato dall'art. 5 del regolamento delegato sia presente e collegato*" al pagamento stesso).
Il prospettato modello operativo si ritiene tuteli con presidi adeguati i fruitori dei servizi di pagamento, dal momento che l'estensione del regime derogatorio è subordinata a specifiche e rigorose condizioni; ma, al contempo, consenta di accedere al sistema e compiere operazioni di pagamento - nell'ambito di una medesima sessione (destinata a chiudersi nel giro di pochi minuti, come ricordato dall'EBA) - in maniera più semplice e rapida.

In conclusione, il Collegio di Coordinamento enuncia il seguente principio di diritto.
"*E' conforme al quadro normativo di riferimento la procedura adottata dall'intermediario che consente ai clienti di accedere al conto con un unico fattore di autenticazione (in applicazione del regime di esenzione di cui all'art. 10 del Regolamento Delegato (UE) 2018/389) e di eseguire un'operazione di pagamento riutilizzando detto fattore insieme con un secondo elemento di autenticazione (di diversa natura), a condizione che: a) l'accesso e il pagamento avvengano nella stessa* sessione; b) *l'associazione dei fattori utilizzati produca il* dynamic linking *(di cui all'art. 5 degli RTS* - Regulatory Technical Standards*/PSD2 -); c) non si tratti del primo accesso al conto da parte dell'utente (nel qual caso è necessaria l'adozione della SCA); d) non siano decorsi più di 180 giorni dall'ultima applicazione della SCA*".

Applicato il principio sopra enunciato al caso in esame, si deve ritenere conforme alla normativa vigente in materia di SCA il procedimento adottato dall'intermediario resistente per consentire l'accesso al conto della cliente, prodromico all'esecuzione dei due pagamenti disconosciuti. Dalla documentazione versata in atti si evince, infatti, che l'accesso è avvenuto con l'inserimento di un solo fattore di autenticazione (*username* e *password*) in quanto nei 180 giorni precedenti vi era stato un precedente accesso eseguito mediante l'impiego di un doppio fattore di autenticazione.
Risulta essere ugualmente coerente con il sopra descritto quadro normativa la procedura seguita dall'intermediario per autorizzare la prima operazione rivelatasi fraudolenta. Dalle evidenze prodotte risulta, in effetti, che per disporre il bonifico di € 4.225,77 è stato riutilizzato il fattore di conoscenza (*username* e *password*) impiegato per l'accesso in combinazione con un OTP (fattore di possesso) inviato via SMS al numero di telefono associato al *device* della parte ricorrente (la quale ha dichiarato - in sede di denuncia - di avere ricevuto l'SMS e di aver autorizzato l'operazione con l'inserimento della causale).
Quanto alla seconda operazione disconosciuta (pagamento di *e-commerce* di € 850,00), nelle controdeduzioni l'intermediario precisa che per autorizzare un'operazione di pagamento *online* con carta di debito sono necessari i seguenti passaggi: accesso all'area riservata mediante *username* e *password*, creazione del CVV dinamico tramite inserimento di un codice OTP inviato via SMS al *device* del cliente, immissione delle credenziali della carta (PAN, data di scadenza e CVV dinamico precedentemente creato), conferma dell'operazione di pagamento mediante un ulteriore OTP ovvero tramite *token*. Tale descrizione trova corrispondenza nei *log* allegati che mostrano la creazione (alle

ore 10:23:25) di un CVV dinamico della carta di debito mediante doppio fattore di autenticazione (inserimento di *username* e *password*) e digitazione del codice OTP ricevuto mediante SMS sul *device* della cliente alle ore 09:23:42; di seguito, alle ore 10:25:25, è stata eseguita l'operazione di pagamento *e-commerce* di € 850,00 mediante inserimento delle credenziali statiche della carta e del codice CVV dinamico, nonché di un codice OTP inviato via SMS. Secondo l'intermediario il procedimento adottato garantirebbe il "*rispetto dell'autenticazione forte*", posto che "*l'inserimento del CVV dinamico è il primo fattore (fattore di conoscenza o di inerenza che è incluso nel processo di generazione del medesimo CVV), mentre la OTP è il secondo fattore (fattore di possesso)*".

Con riguardo alla natura del CVV dinamico quale fattore di autenticazione, il Collegio di Milano - come evidenziato in premessa - rimette la decisione al Collegio di Coordinamento, poiché, "*tenuto conto delle modalità descritte dall'intermediario resistente ed evidenziate dalla documentazione in atti, con le quali si genera il CVV dinamico (mediante l'inserimento della password e dell'OTP) […], ritiene che - pur in assenza di un contrasto tra i vari Collegi territoriali - assum[a] grande rilievo la questione in ordine all'eventuale rilevanza da attribuire al fattore di conoscenza (password) che entra a far parte del più complesso procedimento di generazione del predetto CVV, ai fini della configurabilità o meno di un valido sistema di autenticazione a doppio fattore"*.
In realtà, diversamente da quanto affermato dall'ordinanza di rimessione, nella più recente giurisprudenza dell'Arbitro si possono riscontrare due differenti orientamenti: l'uno che ritiene l'utilizzo del CVV dinamico rientrante in una modalità autorizzativa conforme alla SCA (così, Coll. Roma, dec. 8237/2025; Coll.Torino, dec. 5101/2025; dec. 1709/2025; Coll. Napoli, dec. 3006/2025; Coll. Bari, dec. 7097/2025; Coll. Palermo, dec. 7200/2025); l'altro che è invece dell'opposto parere (in tal senso, Coll. Bologna, dec. 2856/2025; Coll. Milano, dec. 5970/2025; dec. 3619/2025; dec. 3554/2024; dec. 8153/2024; Coll. Palermo, dec. 2775/2025; dec. 2318/2025). In questa prospettiva, riveste ancora più importanza la questione sottoposta a questo Collegio.

Circa il quadro normativo di riferimento in relazione alla natura del CVV assumono rilievo le indicazioni dell'EBA offerte nella *Opinion* del 21.06.2029 e nella risposta alla *Question* ID 2018_4135. Nel primo documento l'Autorità, ricordato che la SCA deve essere assicurata in ogni fase del processo in cui si svolge un'operazione di pagamento e che essa si realizza con il ricorso ad almeno due dei tre fattori di autenticazione appartenenti a categorie diverse (conoscenza; inerenza; possesso), di ciascuno fornisce una esemplificazione coerente con il dettato normativo. Con riguardo al fattore "possesso" (qualificato all'art. 4(30) della PSD2 come "*qualcosa che solo l'utente possiede*") chiarisce che esso - conformemente alle disposizioni di cui all'art. 7 del Regolamento delegato (UE) 2018/389) - non si riferisce soltanto ad un elemento di carattere fisico, potendosene fornire la prova anche attraverso il ricorso ad ogni mezzo affidabile che permetta "*la generazione o la ricezione di un elemento di validazione dinamica sul dispositivo*" (par. 25). In relazione al CVV vengono distinte tre ipotesi: (i) se il CVV è stampigliato sulla carta, non costituisce valido fattore di autenticazione; (ii) se il CVV è dinamico può costituire fattore di possesso; (iii) se viene inviato separatamente al PSU è da equipararsi ad un codice PIN per una nuova carta e potrebbe configurarsi come fattore di conoscenza. In occasione dei lavori di consultazione ai fini dell'*Opinion* del 2019, l'Autorità afferma altresì che la finalità del CVV dinamico è quella di ridurre il rischio frodi, ponendosi come presidio aggiuntivo rispetto agli elementi

dell'autenticazione forte, classificati come possesso, il che non esclude, ma anzi presuppone la sua valenza quale fattore di autenticazione. Posto che i dati devono essere "volatili" per essere considerati elementi di possesso, si ritengono tali i valori dinamici che cambiano grazie all'uso del dispositivo fisico: la circostanza che il CVV dinamico sia generato grazie all'SMS ricevuto sullo *smartphone* permetterebbe quindi di qualificarlo come elemento di possesso. Analoga impostazione si ritrova nella *Question* ID 2028_4135, in cui l'EBA specifica che il CVV costituisce elemento di possesso e non può costituire elemento di conoscenza ("*In addition, while a card with a dynamic card security code may constitute a possession element, it would not constitute a knowledge element*").

Tali indicazioni offerte in prospettiva generale ed astratta dall'EBA sono state recepite da numerosi Collegi territoriali che hanno quindi considerato quale elemento di possesso il CVV dinamico utilizzato per autorizzare le operazioni in seguito disconosciute. Tale qualificazione ha portato a non riconoscere conforme alla SCA il sistema adottato dall'intermediario, in quanto anche il secondo fattore richiesto per procedere all'esecuzione dei pagamenti (il codice OTP ricevuto tramite SMS sul numero di cellulare del cliente) configura un elemento di possesso e, dunque, è della stessa natura, in contrasto con le indicazioni dall'EBA, secondo cui l'autenticazione forte presuppone il ricorso a due fattori appartenenti a categorie differenti.
Occorre peraltro evidenziare che l'EBA ha fornito delle indicazioni di carattere generale, il che implica la necessità di esaminare in concreto gli specifici caratteri del procedimento autorizzativo adottato dall'intermediario riguardandolo nel suo complesso. Del resto, è la stessa Autorità che, nel rispondere alla *Question*ID 4141_2018 sull'accesso informativo (di cui si è sopra detto), impone di considerare complessivamente il sistema di autenticazione e di ritenerlo adeguato se l'associazione di entrambi i fattori utilizzati produca il *dynamic linking* richiesto dall'art. 5 del Regolamento Delegato.
In tale prospettiva, ai fini della configurabilità o meno di un valido sistema di autenticazione a doppio fattore nei casi di utilizzo di CVV dinamico, occorre guardare al procedimento di autorizzazione nel suo complesso. Laddove, come nella fattispecie in esame, il CVV dinamico viene generato previo accesso all'area personale del cliente tramite *username* e *password* ed inserimento di un OTP inviato tramite SMS all'utente, si deve attribuire rilievo al fattore di conoscenza o inerenza (la *password*) che entra a far parte dell'articolato *iter* per produrre il predetto CVV. Da ciò consegue non solo che la generazione del CVV dinamico prevede l'uso di due diversi fattori, uno di conoscenza (la *password*) e uno di possesso (l'OTP), ma anche che il CVV può essere qualificato come fattore di conoscenza, valorizzandosi il riutilizzo di un fattore di autenticazione in fase di accesso avente tale carattere. Deve, conseguentemente, ravvisarsi la conformità a SCA del sistema di autenticazione predisposto dall'intermediario per le operazioni con carta che impieghi quali fattori di autenticazione un CVV dinamico (fattore di conoscenza) e un OTP trasmesso via SMS al numero associato al conto del cliente (fattore di possesso).

In conclusione, il Collegio enuncia il seguente principio di diritto.
"*Configura un sistema di autenticazione a doppio fattore (SCA), come richiesto dalle disposizioni vigenti per autorizzare le operazioni di pagamento, l'utilizzo di un cd. CVV dinamico, generato nella fase di accesso all'area riservata del cliente, accompagnato dall'inserimento di un OTP inviato via SMS*".

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Accertato che l'intermediario ha assolto all'onere di dimostrare che le due operazioni contestate sono state regolarmente autenticate, eseguite e contabilizzate, si può rilevare come lo stesso abbia anche specificamente provveduto "*ad indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell[e] operazion[i] dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente*" (così, Collegio di Coordinamento, dec. 22745/19, in relazione all'interpretazione della "*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*").

Sulla base di quanto esposto dalla parte ricorrente (come sopra riportato) e della documentazione dalla stessa prodotta, può ritenersi che sia stata vittima di una frode qualificabile come *SMS/spoofing*, avendo ricevuto un messaggio - circa una presunta operazione da lei non autorizzata - in apparenza proveniente dall'intermediario convenuto, che l'aveva indotta ad attenuare la sua soglia di attenzione e a prestare fede alla comunicazione pervenutale. In effetti, la denominazione della *chat* in cui è inserito il messaggio civetta parrebbe riferibile all'intermediario; il detto messaggio contiene però errori grammaticali e di punteggiatura che avrebbero dovuto allertarla circa la non riconducibilità dello stesso alla sua banca; analoghi caratteri hanno successivi messaggi relativi a blocchi cautelativi del conto corrente.
Quanto all'utenza indicata nell'SMS che la ricorrente ha contattato per avere informazioni in merito alla presunta disposizione di un bonifico di € 199,00, essa non è in alcun modo riferibile all'intermediario (da una verifica della Segreteria Tecnica del Collegio di Milano il numero risulterebbe essere segnalato in Internet come collegato a truffe). Oltre a questi comportamenti già connotati da colpa grave, si deve altresì rilevare, come evidenzia l'intermediario convenuto, che la ricorrente abbia comunicato ad un terzo sconosciuto (sia pure qualificatosi come sedicente operatore dell'ufficio frodi della banca) i codici OTP ricevuti e non abbia prestato attenzione alla mancata ricezione di una notifica in *app* nella sezione "*I miei messaggi*" indicativa del fatto che non era stata contatta dalla propria banca.
Appare inoltre totalmente irrealistico poter pensare che per bloccare un addebito non autorizzato si debba provvedere ad eseguire un'operazione di pagamento. Alla luce di quanto sopra esposto, il Collegio ritiene gravemente colposa la condotta della parte ricorrente, anche in relazione agli obblighi di cui all'art. 7, comma 3 del d. lgs. n. 11/201. Per converso, nessuna responsabilità è ravvisabile in capo all'intermediario resistente, tenutosi altresì conto che le due differenti operazioni di pagamento non integrano alcun parametro di cui all'art. 8, rubricato "*Rischio di frode*", del D.M. 30.04.2007, n. 112 (Regolamento di attuazione della l. n. 166/2005, sulla "*Istituzione di un sistema di prevenzione delle frodi di pagamento*").

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE