COLLEGIO DI COORDINAMENTO

composto dai signori:

(CO) MAUGERI	Presidente
(CO) CARRIERO	Membro designato dalla Banca d'Italia
(CO) LUCCHINI GUASTALLA	Membro designato dalla Banca d'Italia
(CO) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(CO) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore: CIPRIANI

Seduta del 10/07/2024

FATTO

A. La ricorrente, titolare di una carta di credito gestita dall'intermediario, si rivolge all'Arbitro illustrando di essere stata contattata il 10.10.2023 da un operatore della resistente, il quale le chiedeva conferma dell'ordine di disposizione di un pagamento online di € 816,90. Disconosciuta l'operazione, la ricorrente verificava che, nel periodo compreso tra il 24.9.2023 e il 5.10.2023, erano state effettuate con la sua carta di credito dieci operazioni da lei non autorizzate, per un esborso totale di € 8.160,01. Pertanto, la ricorrente chiede il rimborso della somma in questione.
B. L'intermediario, costituitosi, ha eccepito preliminarmente l'inammissibilità del ricorso in ragione della incompletezza della ricostruzione dei fatti e di una finalità sostanzialmente consulenziale. Nel merito, ha fatto presente che il 3.09.2023 (ventuno giorni prima della prima operazione contestata) la ricorrente aveva ricevuto un SMS truffaldino con il quale era stata indotta ad aprire un link e a compilare un modulo. Al termine della procedura, la ricorrente aveva ricevuto un ulteriore SMS che la informava dell'avvenuta attivazione della carta ad A**** Pay, ma, nonostante questo, non si era allarmata né aveva ritenuto di mettersi in contatto con la resistente per chiedere spiegazioni.
Quanto alle operazioni contestate, l'intermediario ha precisato che esse sono state effettuate tramite *digital wallet* e ha dedotto la loro corretta autenticazione tramite

procedura conforme a quanto richiesto dalla normativa sulla Strong Costumer Authentication (SCA).
Infine, l'intermediario ha dedotto di avere già provveduto a stornare una operazione dell'importo di € 1.124,00 che andrebbero dunque in ogni caso sottratti dalle somme richieste dalla ricorrente.
C. Il Collegio di Roma, investito della decisione, superata l'eccezione di inammissibilità del ricorso, ha acclarato in particolare quanto segue:
i) Le operazioni in questione sono state effettuate previa tokenizzazione della carta nel wallet presente su un cellulare del truffatore, autorizzata "con inserimento della password (fattore di conoscenza) e riconoscimento biometrico (fattore di inerenza)".
ii) "Le successive operazioni dispositive risultano effettuate con la carta tokenizzata su wallet A**** Pay e autorizzate con impiego del dispositivo certificato (fattore di possesso) e di un passcode definito dall'utente, che l'intermediario qualifica come fattore di conoscenza, e che corrisponde al codice di sblocco del dispositivo".
Tanto premesso, il Collegio di Roma da un lato ha rilevato la sussistenza dei fattori di autenticazione forte nella operazione di associazione della carta al wallet. Dall'altro lato, però, dubita della conformità a SCA del procedimento di autorizzazione delle singole operazioni di pagamento, in particolare ponendo la questione della possibilità di considerare quale valido fattore rilevante ai fini della SCA – segnatamente, quale fattore di conoscenza – il codice di sblocco del dispositivo. In particolare, il Collegio di Roma richiama una Opinion dell'EBA (Q&A 2021_6145), nella quale – con riferimento alla fase della tokenizzazione della carta - si è ritenuto che lo sblocco del dispositivo mediante face-id, o pin/password non dovrebbe essere considerato un elemento SCA valido ai fini dell'aggiunta di una carta di pagamento a un portafoglio digitale se il meccanismo di blocco dello schermo del dispositivo mobile non è sotto il controllo dell'emittente o se il pagatore non è stato associato precedentemente tramite una SCA con le credenziali utilizzate per sbloccare il telefono.
Il Collegio rimettente segnala inoltre il rischio che "una volta sbloccato lo smartphone mediante l'inserimento del codice, fingerprint o riconoscimento biometrico che serve a questo fine, il device potrebbe essere utilizzato per autorizzare un numero indefinito di operazioni di pagamento mediante un solo fattore di autenticazione, ossia quello del suo possesso", il che farebbe dubitare della conformità a SCA dell'operazione.
Pertanto, anche in considerazione di alcune difformità nei precedenti dei Collegi territoriali, in ragione della particolare importanza della questione e al fine di evitare contrasti interpretativi, il Collegio di Roma ha rimesso l'esame del ricorso al Collegio di coordinamento.

DIRITTO

1. La controversia concerne una vicenda di uso non autorizzato di uno strumento di pagamento, nella specie consistente in alcuni pagamenti effettuati mediante carta di credito previamente "tokenizzata" su un telefono cellulare e poi utilizzata attraverso il digital wallet installato sul medesimo apparecchio.
2. In via preliminare, va esaminata l'eccezione sollevata da parte resistente, a parere della quale il ricorso si presenterebbe "oscuro e confuso", al punto da meritare la sanzione dell'inammissibilità. Sul punto, come già rilevato dal Collegio rimettente, si deve osservare che, sebbene parte ricorrente non descriva nei dettagli le modalità esecutive della frode subita, *petitum* e *causa petendi* del ricorso risultano nel complesso ben chiari, non sussistendo dubbi sul fatto che oggetto del ricorso sia la richiesta di rimborso di alcune specifiche operazioni disconosciute. L'eccezione preliminare dell'intermediario, pertanto, non può trovare accoglimento.

3. Nel passare all'esame del merito, la ricorrente chiede il rimborso di alcune operazioni disconosciute in quanto eseguite fraudolentemente da terzi.
4. Il Collegio rileva innanzi tutto che l'operazione contestata è stata eseguita sotto il vigore del d.lgs. 27.1.2010, 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 13.1.2018. Inoltre, l'operazione contestata è stata eseguita successivamente all'entrata in vigore delle nuove 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).
5. La disciplina appena 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 (artt. 7 e 12, co. 4, d.lgs. n. 11/2010).
In particolare, "qualora l'utente 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" (ai sensi dell'art. 10, d.lgs. n. 11/2010). Inoltre, ove l'utente 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'utente 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. 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" (art. 10 comma 2, d.lgs. cit.).
Ai sensi del successivo art. 12, co. 2 bis, d.lgs. cit., "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).
I prestatori di servizi di pagamento sono tenuti a utilizzare l'autenticazione forte "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" (art. 97, comma 1, direttiva UE 2015/2366; art. 10-bis, comma 1, d.lgs. 11/2010).
In relazione alla disciplina richiamata, 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 non superiore a 50 euro). 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. Coord., decisione n. 3947 del 24.6.2014. Più di recente, cfr. Coll. Coord., decisione 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, co. 2, d. lgs. n. 11/2010).

Ai fini della decisione del presente ricorso, inoltre, viene in rilievo la disciplina dettata dall'art. 24 del Regolamento Delegato n. 389/2018, per il quale "I prestatori di servizi di pagamento assicurano che solo l'utente dei servizi di pagamento sia associato, in modo sicuro, alle credenziali di sicurezza personalizzate, ai dispositivi e al software di autenticazione" (comma 1); e "l'associazione tramite un canale a distanza dell'identità dell'utente dei servizi di pagamento alle credenziali di sicurezza personalizzate e ai dispositivi o al software di autenticazione è effettuata ricorrendo all'autenticazione forte del cliente" (comma 2, lett. b).

6. Fatta questa doverosa premessa, venendo al caso oggi sottoposto all'esame del Collegio di coordinamento, si deve rilevare che nella specie – come già si è accennato - tutte le operazioni contestate sono state eseguite mediante digital wallet. Ciò ha richiesto preliminarmente la tokenizzazione della carta sul wallet installato sul dispositivo del truffatore; poi, l'esecuzione dei singoli pagamenti.

Orbene, non è in discussione il fatto che sia la tokenizzazione dello strumento di pagamento sia i successivi pagamenti effettuati mediante wallet richiedano, in virtù dell'art. 10-bis, comma 1, d.lgs. 11/2010, la procedura di autenticazione forte. Pertanto, di fronte al disconoscimento delle operazioni di pagamento effettuato dall'utente, si deve innanzi tutto verificare che l'intermediario abbia assolto l'onere, posto a suo carico dall'art. 10, d.lgs. 11/2011, di dimostrare che l'operazione di pagamento è stata effettuata mediante uso della SCA in tutte le fasi rilevanti.

Dalle evidenze prodotte dall'intermediario e dalla legenda allegata, si evince che il 3/9/2023, alle 15.26, è stato eseguito l'accesso all'app dell'intermediario con contestuale certificazione di un nuovo dispositivo, autorizzata tramite username e password (fattore di conoscenza), nonché OTP SMS inviato sul numero della ricorrente (fattore di possesso); con le medesime modalità è stato inoltre attivato il riconoscimento biometrico sul nuovo dispositivo; subito dopo, alle 15.29, è stata eseguita la tokenizzazione della carta della ricorrente su wallet A**** Pay, anch'essa autorizzata con inserimento della password (fattore di conoscenza) e riconoscimento biometrico (fattore di inerenza).

Le successive operazioni di disposizione dei singoli pagamenti sono poi state effettuate tutte con la carta tokenizzata sul wallet A*** Pay e autorizzate con il dispositivo certificato

(fattore di possesso), nonché con digitazione del codice di sblocco del dispositivo, che l'intermediario qualifica come fattore di conoscenza.
Nella specie, l'intermediario ha fornito adeguata prova, anche mediante deposito dei log delle relative operazioni, dell'effettivo uso dei predetti fattori di autenticazione in tutti i passaggi evidenziati.
7. In questa situazione, va innanzi tutto condiviso il rilievo del Collegio rimettente, che ha ritenuto conforme a SCA la procedura di associazione della carta al wallet, nella specie effettuata attraverso la app della banca e mediante l'uso di un fattore di conoscenza (credenziali statiche) per sbloccare l'App e un fattore di possesso (SMS OTP) per il completamento della procedura.
8. Per quanto riguarda invece le singole operazioni di pagamento, come si è illustrato, esse risultano autorizzate con il dispositivo certificato nonché con digitazione del codice di sblocco del dispositivo. I due fattori rilevanti ai fini della SCA sarebbero quindi: il possesso, rappresentato dalla disponibilità del dispositivo abilitato; e la conoscenza, rappresentata dal codice di sblocco del dispositivo.
Il Collegio rimettente non dubita del fatto che l'uso del dispositivo certificato con la carta tokenizzata costituisca valido fattore di possesso: come ha avuto modo di chiarire anche l'EBA nella Q&A ID 2019_4827, una volta tokenizzata la carta, l'utilizzo dello strumento integra fattore di possesso, purché il prestatore di servizi di pagamento sia stato direttamente o indirettamente coinvolto nel processo di rilascio del token, in modo da consentire la verifica dell'identità dell'utilizzatore e l'associazione del token a un device affidabile. Nella specie, la tokenizzazione della carta (consentita in virtù di apposito accordo sottoscritto tra il gestore del wallet e la resistente, quale emittente della carta) è avvenuta a partire dalla App dell'intermediario, sí che il suo coinvolgimento diretto nel processo di rilascio del token non è revocabile in dubbio.
9. Per converso, il Collegio di Roma esprime un dubbio in ordine all'idoneità del passcode del dispositivo a costituire, come sostiene l'intermediario, valido fattore di conoscenza. Segnatamente, come si è accennato, il rimettente rileva che sul punto sussisterebbe un atteggiamento non uniforme dei Collegi di merito: alcuni (Collegio di Milano, decisione n. 6138/2023) hanno ritenuto il passcode quale valido fattore di autenticazione; altri (Collegio di Roma, decisioni n. 1648/2024 e 13429/2023) sono giunti a conclusione diversa, in particolare richiamando una Opinion dell'EBA (Q&A 2021_6145), che aveva ritenuto non idoneo il passcode quale fattore di autenticazione nella fase (diversa da quella del pagamento, come del resto sottolinea lo stesso Collegio rimettente) della tokenizzazione della carta.
Inoltre, il Collegio di Roma osserva anche che "lo sblocco di operatività dello *smartphone* prescinde dall'inserimento di una specifica operazione di pagamento che debba essere autenticata, in particolare per quanto riguarda il suo importo e il suo beneficiario. In altri termini, una volta sbloccato lo smartphone mediante l'inserimento del codice, *fingerprint* o riconoscimento biometrico che serve a questo fine, il device potrebbe essere utilizzato per autorizzare un numero indefinito di operazioni di pagamento mediante un solo fattore di autenticazione, ossia quello del suo possesso".
10. Orbene, il Collegio di coordinamento ritiene utile avviare l'analisi proprio dall'esame dell'Opinion EBA Q&A 2021_6145. Infatti, per quanto le opinioni espresse dall'EBA non debbano considerarsi vincolanti, costituendo soltanto un riferimento utilizzabile in sede interpretativa, nel caso di specie pare rilevante definire con precisione l'ambito in riferimento al quale il parere sopra richiamato è stato espresso.
Nella specie, era stato posto all'EBA un quesito sulla possibilità di considerare il passcode per sbloccare il dispositivo mobile come uno degli elementi di autenticazione forte del cliente quando un utente di un servizio di pagamento tokenizza una carta su una soluzione

di portafoglio elettronico come A**** Pay (lo stesso usato nel caso in esame). Orbene, l'EBA ha chiarito che il passcode "non dovrebbe essere considerato un elemento SCA valido ai fini dell'aggiunta di una carta di pagamento a un portafoglio digitale se il meccanismo di blocco dello schermo del dispositivo mobile non è sotto il controllo dell'emittente o se il pagatore non è stato associato precedentemente tramite una SCA con le credenziali utilizzate per sbloccare il telefono".
Dunque, va sottolineato da un lato che l'Opinion dell'EBA riguarda il caso specifico dell'uso del passcode nella fase della tokenizzazione; dall'altro che nel parere si è comunque ritenuto che la preventiva associazione del pagatore tramite SCA con le credenziali utilizzate per sbloccare il telefono consenta, in seguito, di utilizzare il codice di sblocco quale valido fattore di conoscenza.
11. Questa impostazione ha trovato riscontro nelle decisioni dei Collegi territoriali dell'Arbitro. Sul punto, le difformità segnalate dal Collegio rimettente sono, a parere del Collegio di coordinamento, da ridimensionare. Infatti, il Collegio di Milano (cfr. decisione 6138/2023) ha ritenuto conformi a SCA i pagamenti effettuati mediante wallet e approvati con "il possesso del dispositivo su cui sono presenti i wallet (elemento di possesso) e il passcode (elemento di conoscenza)". Anche il Collegio di Roma (decisione n. 13399/2023) è giunto a una analoga conclusione, in particolare valorizzando il fatto che nel caso di specie il prestatore di servizi di pagamento risultasse coinvolto "nel processo di rilascio del token, in quanto […] l'OTP che consente l'associazione della carta al wallet è stata inviata all'utenza previamente registrata dal cliente presso il prestatore di servizi di pagamento".
Peraltro, in due casi, come segnala il Collegio rimettente, lo stesso Collegio di Roma ha ritenuto non provata la SCA in relazione a operazioni effettuate tramite wallet (decisioni nn. 1648/2024 e 13429/2023). Tuttavia, in entrambi le ipotesi, a veder bene la ragione della decisione va individuata nella insufficienza della documentazione prodotta dall'intermediario, in particolare in relazione alla fase (precedente a quella del pagamento, e oggetto della già richiamata Opinion dell'EBA 2021_6145) della tokenizzazione: tale deficit documentale non ha consentito di appurare la previa associazione del passcode all'utente tramite una procedura adeguata in fase di tokenizzazione, il che ha poi prodotto conseguenze sulla successiva utilizzabilità del passcode.
In altre parole, non pare che i Collegi territoriali abbiano mai escluso la validità del passcode a fungere da fattore di conoscenza valido ai fini SCA per i pagamenti effettuati tramite wallet in ipotesi sovrapponibili – anche in termini di apparato probatorio prodotto dall'intermediario – a quella oggi all'esame del Collegio di coordinamento.
12. Invero, la procedura di tokenizzazione della carta, se effettuata tramite SCA, consente di portare il meccanismo di blocco dello schermo del dispositivo mobile (che può essere il passcode o il riconoscimento biometrico) sotto il controllo dell'emittente e per associare il pagatore con la credenziale utilizzata per lo sblocco del device.
Sul punto, è il caso di sottolineare che – quanto meno in un caso come quello oggetto del presente ricorso - l'uso del passcode quale fattore di conoscenza è da considerarsi in tutto e per tutto fungibile con il riconoscimento biometrico quale fattore di inerenza. Infatti, il dispositivo concretamente utilizzato nel caso di specie consente all'utente di sostituire in qualsiasi momento (sia a livello di sistema, sia per la singola operazione) il riconoscimento biometrico con la digitazione del codice.
Pertanto, deve ritenersi che lo sblocco del telefono (o, in alternativa, il riconoscimento biometrico): i) da un lato, non possa essere usato come elemento valido per la SCA durante la tokenizzazione; ii) dall'altro lato, una volta effettuata la tokenizzazione mediante SCA, possa essere usato come elemento della SCA durante le successive operazioni di

pagamento, in quanto l'utente è stato ormai previamente associato tramite SCA alle credenziali usate per lo sblocco del telefono.

13. In definitiva, tornando al caso di specie, la circostanza che il codice di sblocco del cellulare sia stato utilizzato nella fase di tokenizzazione della carta, unitamente a un sistema di autenticazione conforme a SCA, ha consentito di associarlo univocamente all'utente e ha fatto sì che lo stesso codice potesse essere validamente reimpiegato in fase dispositiva.

14. Sotto altro profilo, a parere del Collegio rimettente, l'uso del codice di sblocco dell'apparato come elemento di conoscenza comporterebbe il rischio che, una volta sbloccato lo smartphone mediante passcode, il device potrebbe essere utilizzato per autorizzare un numero indefinito di operazioni di pagamento mediante un solo fattore di autenticazione, ossia quello del suo possesso. Più in particolare, nella specie si sarebbe al di fuori della ipotesi in cui, in caso di avvio di una sessione di pagamento mediante due fattori di autenticazione forte, sarebbe poi possibile tenerne fermo uno per la durata di tale sessione, autorizzando le singole operazioni al suo interno mediante un solo fattore aggiuntivo di autenticazione (in tal senso v. la Q&A ID 2018_4141 dell'EBA). Ciò perché, a parere del Collegio di Roma, "nel caso di cui si tratta […] la sessione di pagamento non sembrerebbe avviata mediante due fattori di autenticazione, ma mediante il solo inserimento del codice, fingerprint o riconoscimento biometrico che sblocca il cellulare: una volta che tale device è stato sbloccato, ciascuna operazione di pagamento parrebbe autorizzata mediante un solo fattore di autenticazione, ossia il possesso".

Invero, il Collegio di Coordinamento ritiene di dover proporre una diversa ricostruzione. In un caso come quello oggi all'esame del Collegio, infatti, la sessione di pagamento deve ritenersi avviata tramite un doppio fattore di autenticazione: il passcode quale fattore di conoscenza (che avrebbe potuto essere sostituito dal riconoscimento biometrico quale fattore di inerenza) e la disponibilità del dispositivo precedentemente autenticato quale fattore di possesso. Questo, all'interno della medesima sessione di pagamento, avrebbe in ogni caso consentito di ritenere possibile tenere fermo il primo fattore di autenticazione (il passcode) e autorizzare gli ulteriori pagamenti con il solo possesso.

Ad ogni modo, nella specie non vi è necessità di invocare la predetta eccezione, in quanto dalla documentazione prodotta dall'intermediario risulta che per tutti i singoli pagamenti (effettuati tra l'altro non in sequenza ma a distanza di tempo l'uno dall'altro, quindi in diverse sessioni di pagamento), oltre al possesso, è stato acquisito anche il secondo fattore, rappresentato per l'appunto dal passcode. Del resto, la documentazione tecnica relativa al funzionamento del digital wallet nella specie utilizzato (A**** pay) porta a ritenere che sia richiesto sempre il secondo fattore di autenticazione (inerenza/conoscenza).

15. In definitiva, il Collegio di coordinamento ritiene di dover enunciare il seguente principio di diritto:

Nell'autenticazione di operazioni di pagamento tramite digital wallet, il codice di sblocco del dispositivo utilizzato (ovvero, in alternativa, il riconoscimento biometrico) può valere come secondo fattore rilevante ai fini della SCA, purché esso sia stato in via preventiva associato univocamente all'utente, mediante uso nella fase di tokenizzazione dello strumento all'interno del wallet, con procedura conforme a SCA.

16. Alla luce di quanto sopra illustrato, può ritenersi che l'intermediario abbia adempiuto all'onere probatorio posto a suo carico dall'art. 10, comma 1, d.lgs. 11/2010.

Peraltro, come si è illustrato, questo non consente di porre automaticamente le operazioni contestate a carico del cliente, dovendosi comunque verificare la sussistenza di una sua colpa grave o dolo (Collegio di Coordinamento, decisione 22745/2019).

Orbene, il Collegio ritiene che nella specie effettivamente sussista una colpa particolarmente grave della ricorrente.
Infatti, dalle allegazioni delle parti e dalla documentazione prodotta può considerarsi dimostrato che nella specie la ricorrente ha ricevuto un sms "civetta" sulla medesima chat abitualmente utilizzata dall'intermediario; ha cliccato sul link contenuto nell'sms e ha fornito le proprie credenziali e comunicato il successivo SMS OTP al truffatore; ha poi ricevuto un ulteriore SMS che le confermava l'attivazione della sua carta sul wallet "A**** pay" senza porsi il problema di contattare l'intermediario per chiedere spiegazioni.
In questa situazione, il fatto che il primo sms fosse contenuto nella chat dell'intermediario costituisce un elemento che rende la truffa particolarmente sofisticata e che in parte potrebbe giustificare l'aver dato seguito al link in esso contenuto. Tuttavia, nel concreto svolgimento della vicenda, l'inerzia di fronte al successivo messaggio di conferma dell'attivazione della carta sul wallet ha costituito un elemento assolutamente decisivo, la cui autonoma efficienza causale ai fini della riuscita della truffa è stata tale da far ritenere sussistente la colpa grave della ricorrente e da porre a suo carico tutte le conseguenze dannose della vicenda.
Il ricorso, pertanto, non risulta meritevole di accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

LA PRESIDENTE

Firmato digitalmente da
MARIA ROSARIA MAUGERI