DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

SCA, riutilizzo dei fattori e CVV dinamico

Note ad ABF, Collegio di coordinamento, n. 4274/2026

Giugno 2026

Fabrizio Cascinelli, Partner, PwC Legal
Luca Bettinelli, Senior Manager, PwC Legal

Fabrizio Cascinelli, Partner, PwC Legal

Luca Bettinelli, Senior Manager, PwC Legal

Fabrizio Cascinelli

Fabrizio Cascinelli è Partner del dipartimento Banking and Finance di PwC Legal e referente dello studio per il mercato Financial Services. Assiste banche, intermediari finanziari, istituti di pagamento e di moneta elettronica, imprese di assicurazione e altri operatori vigilati su tematiche di regolamentazione bancaria, finanziaria e assicurativa.

Luca Bettinelli

Luca Bettinelli è Senior Manager nel dipartimento Banking and Finance di PwC Legal, dove assiste banche, imprese di investimento, istituti di pagamento e di moneta elettronica, nonché altri intermediari vigilati, su tematiche di regolamentazione bancaria e finanziaria.

Società tra Avvocati

PwC Legal

1. Le questioni decise e la tesi del commento

La Decisione n. 4274 del 12 maggio 2026 risolve due contrasti emersi nei Collegi territoriali dell'Arbitro Bancario Finanziario.

Il primo riguarda il rapporto tra l'esenzione prevista dall'art. 10 del Regolamento delegato (UE) 2018/389 e la successiva disposizione di un pagamento. L'art. 10 consente al prestatore di servizi di pagamento di non applicare l'autenticazione forte quando il cliente accede direttamente al conto soltanto per consultare il saldo o le operazioni degli ultimi novanta giorni, purché non siano mostrati dati sensibili relativi ai pagamenti; la SCA resta comunque necessaria al primo accesso e quando siano trascorsi più di centottanta giorni dall'ultima autenticazione forte.[1] Il Collegio ammette che il fattore utilizzato per tale accesso informativo possa essere riutilizzato, nella stessa sessione, per la successiva operazione, purché al momento del pagamento venga applicato un secondo elemento appartenente a una categoria diversa e sia assicurato il dynamic linking.

Il secondo contrasto riguarda il CVV dinamico. Il Collegio considera conforme alla SCA una procedura nella quale il codice viene generato nell'area riservata attraverso password e OTP e viene poi utilizzato, insieme a un ulteriore OTP, per confermare un pagamento e-commerce. La decisione qualifica il CVV come elemento di conoscenza valorizzando la password utilizzata nel procedimento di generazione.

Le due soluzioni richiedono valutazioni distinte. La prima è condivisibile: né la direttiva (UE) 2015/2366 (PSD2) né il Regolamento delegato impongono che i due fattori siano digitati nello stesso momento. Il pagamento resta soggetto a SCA, ma il fattore già validato può essere riutilizzato se la sessione è ancora tecnicamente attiva e il secondo elemento viene applicato alla specifica operazione.

La seconda soluzione è più problematica, occorrendo stabilire se un codice normalmente riconducibile al possesso possa essere qualificato come conoscenza soltanto perché una password è stata utilizzata

1 Art. 10 del Regolamento delegato (UE) 2018/389, come modificato dal Regolamento delegato (UE) 2022/2360. La disposizione consente di non applicare la SCA se l'accesso diretto al conto è limitato al saldo o alle operazioni eseguite negli ultimi novanta giorni, senza divulgazione di dati sensibili relativi ai pagamenti. L'esenzione non opera al primo accesso né quando sono trascorsi più di centottanta giorni dall'ultima applicazione della SCA.

vedi l'articolo online

a monte per generarlo. Il commento propone di distinguere tre elementi: la password, che costituisce il fattore originario; il procedimento attraverso il quale il codice viene generato; il CVV dinamico, che è il risultato di tale procedimento. La natura del risultato non coincide necessariamente con quella di tutti i fattori impiegati per produrlo.

2. La vicenda e le questioni rimesse al Collegio di coordinamento

La controversia trae origine da una frode realizzata attraverso la combinazione di SMS spoofing e vishing. La cliente riceveva un messaggio apparentemente proveniente dalla propria banca, nel quale veniva informata dell'avvenuta disposizione di un bonifico di euro 199 e invitata a contattare un numero telefonico qualora non riconoscesse l'operazione. Convinta dell'autenticità della comunicazione, chiamava il numero indicato e veniva messa in contatto con un soggetto qualificatosi come addetto dell'ufficio antifrode.

Il falso operatore, dopo averle chiesto una parte della password di accesso all'home banking, le rappresentava l'esistenza di ulteriori addebiti anomali e la necessità di mettere in sicurezza il conto. In tale contesto, la cliente accedeva alla propria area riservata e, seguendo le istruzioni ricevute, trasferiva euro 4.225,77 verso un conto indicato dal truffatore come conto sicuro. Successivamente veniva indotta a compiere un'ulteriore operazione di euro 850, che riteneva funzionale al blocco di altri addebiti e che si rivelava, invece, un pagamento e-commerce effettuato mediante la propria carta di debito.

La frode si articolava, pertanto, in due operazioni tecnicamente differenti. La prima consisteva in un bonifico disposto dal dispositivo abitualmente utilizzato dalla cliente. La seconda era un pagamento online con carta, per il quale erano stati utilizzati i dati statici dello strumento, un CVV dinamico precedentemente generato e un ulteriore codice OTP.

L'intermediario sosteneva che entrambe le operazioni fossero state correttamente autenticate, registrate e contabilizzate. Quanto al bonifico, rilevava che la cliente aveva effettuato l'accesso all'home banking mediante username e password e aveva successivamente autorizzato l'operazione mediante un OTP inviato al numero telefonico associato al conto. Quanto al pagamento e-commerce, descriveva una procedura articolata in più fasi: accesso all'area riservata; generazione del CVV dinamico mediante password e OTP; inserimento dei dati della carta e del CVV nel sito del merchant; conferma finale del pagamento mediante un ulteriore OTP.

La ricorrente chiedeva il rimborso integrale delle somme, sostenendo di non avere autorizzato consapevolmente le operazioni e di essere stata vittima di una frode resa credibile dall'apparente provenienza bancaria dei messaggi. L'intermediario opponeva, oltre alla regolarità delle procedure di autenticazione, la colpa grave della cliente, valorizzando la comunicazione delle credenziali, l'esecuzione delle operazioni indicate dal falso addetto e la presenza di plurimi segnali di anomalia.

Il Collegio territoriale riteneva applicabile la disciplina delle operazioni non autorizzate, osservando che il contributo della cliente alla fase dispositiva e autorizzativa appariva soltanto parziale e che il consenso, ai sensi della disciplina speciale sui servizi di pagamento, deve essere prestato nella forma convenuta con il prestatore. L'intermediario era quindi tenuto a dimostrare l'applicazione della strong customer authentication in tutte le fasi rilevanti.

La rimessione al Collegio di coordinamento riguardava due distinti contrasti interpretativi.

Il primo concerneva l'art. 10 del Regolamento delegato (UE) 2018/389, che consente al PSP di non applicare la SCA quando il cliente accede al conto esclusivamente per consultare il saldo o le operazioni recenti, purché non si tratti del primo accesso e non siano trascorsi più di centottanta giorni dall'ultima autenticazione forte. Si trattava di stabilire se il fattore utilizzato per tale accesso informativo potesse essere riutilizzato, nella stessa sessione, ai fini della successiva disposizione di un pagamento, insieme a un secondo elemento di diversa natura.

Il secondo contrasto riguardava il CVV dinamico. L'intermediario sosteneva che il codice, essendo generato attraverso una procedura nella quale erano stati utilizzati password e OTP, potesse essere considerato un elemento di conoscenza e, insieme all'OTP finale, integrare una SCA valida. Parte della giurisprudenza ABF aderiva a tale ricostruzione; un diverso orientamento qualificava invece tanto il CVV dinamico quanto l'OTP come elementi di possesso, con conseguente assenza di due fattori appartenenti a categorie differenti.

La decisione affronta dunque due problemi collegati ma distinti: da un lato, la possibilità di distribuire nel tempo i fattori della SCA all'interno della medesima sessione; dall'altro, la possibilità di attribuire al

vedi l'articolo online

CVV dinamico la natura del fattore utilizzato nel procedimento attraverso cui esso è stato generato.

3. Autenticazione, autorizzazione e SCA nel sistema dei pagamenti

La disciplina dei pagamenti disconosciuti impone di distinguere autenticazione, autorizzazione ed esecuzione tecnica.

L'**autenticazione** è la procedura con cui il PSP verifica l'identità dell'utente o la validità dell'uso di uno specifico strumento, incluse le credenziali di sicurezza personalizzate. L'**autorizzazione** riguarda invece il consenso del pagatore alla singola operazione, espresso nella forma concordata con il prestatore. La corretta registrazione e contabilizzazione dimostrano che l'ordine è transitato nei sistemi, ma non provano, da sole, né il consenso del cliente né la sua colpa.[2]

L'obbligo sostanziale di applicare la strong customer authentication discende dall'art. 97 PSD2, recepito in Italia dall'art. 10-bis del d.lgs. 27 gennaio 2010, n. 11, come modificato e integrato dal d.lgs. 15 dicembre 2017, n. 218; l'art. 98 PSD2 conferisce invece all'EBA il mandato per elaborare gli standard tecnici.[3] La SCA è richiesta, in particolare, quando il cliente accede online al conto, dispone un pagamento elettronico o compie a distanza un'azione che può comportare un rischio di frode.

La procedura deve utilizzare almeno due elementi indipendenti appartenenti a categorie diverse:

i. **conoscenza**, ossia qualcosa che solo l'utente conosce, come una password o un PIN;

ii. **possesso**, ossia qualcosa che solo l'utente possiede o controlla, come un dispositivo sul quale viene ricevuto o generato un codice dinamico;

iii. **inerenza**, ossia qualcosa che caratterizza l'utente, come l'impronta digitale o il riconoscimento facciale.

Non è sufficiente utilizzare due codici diversi: occorre verificare quale funzione svolgano (un CVV dinamico e un OTP possono essere due valori distinti ma appartenere entrambi al possesso). Inoltre, la compromissione di un fattore non deve compromettere l'affidabilità dell'altro.[4]

Per i pagamenti elettronici a distanza si aggiunge il **dynamic linking**. L'utente deve essere informato dell'importo e del beneficiario e il codice di autenticazione deve essere specifico per quei dati; se importo o beneficiario vengono modificati, il codice deve diventare invalido.[5] In termini pratici, non basta dimostrare che un OTP sia stato inviato: il PSP deve provare che il codice fosse riferito proprio a quella transazione.

Il riparto dell'onere della prova è disciplinato dall'art. 10 del d.lgs. n. 11/2010. Quando il cliente nega di avere autorizzato un pagamento, il prestatore deve dimostrare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito malfunzionamenti o altri inconvenienti. La stessa norma precisa che l'utilizzo registrato dello strumento non è necessariamente sufficiente a provare l'autorizzazione, la frode o la colpa grave del cliente.[6]

La SCA costituisce quindi il primo passaggio dell'accertamento. Se l'intermediario non dimostra di avere applicato una procedura conforme, la questione della colpa grave resta automaticamente assorbita,

2 Cfr. artt. 4, punti 29 e 30, e 64 della direttiva (UE) 2015/2366; artt. 1, lett. q-bis), 5, 9 e 10 del d.lgs. 27 gennaio 2010, n. 11. L'autenticazione verifica l'identità o la validità dell'uso dello strumento; l'autorizzazione richiede il consenso del pagatore nella forma concordata con il PSP.

3 Art. 97 della direttiva (UE) 2015/2366 e art. 10-bis del d.lgs. n. 11/2010. L'art. 97 richiede la SCA quando il pagatore accede online al conto, dispone un pagamento elettronico o compie a distanza un'azione che può comportare rischio di frode. L'art. 98 PSD2 conferisce all'EBA il mandato per elaborare gli RTS. Il d.lgs. n. 11/2010 è stato modificato, per il recepimento della PSD2, dal d.lgs. 15 dicembre 2017, n. 218.

4 Art. 4, punto 30, PSD2; artt. 4 e 6-9 del Regolamento delegato (UE) 2018/389. I fattori devono appartenere ad almeno due categorie tra conoscenza, possesso e inerenza ed essere indipendenti, in modo che la compromissione dell'uno non pregiudichi l'affidabilità dell'altro.

5 Art. 97, par. 2, PSD2 e art. 5 del Regolamento delegato (UE) 2018/389. Il codice di autenticazione deve essere specifico per importo e beneficiario; il pagatore deve poter conoscere entrambi e qualsiasi modifica deve invalidare il codice.

6 Art. 10, commi 1 e 2, del d.lgs. n. 11/2010. Il PSP deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito malfunzionamenti; la sola registrazione dell'uso dello strumento non è necessariamente sufficiente a provare autorizzazione, frode o colpa grave. V. anche ABF, Collegio di coordinamento, 10 ottobre 2019, n. 22745.

salvo il comportamento fraudolento del pagatore.[7]

4. L'esenzione dell'art. 10 RTS e il riutilizzo del fattore nella medesima sessione

4.1 *Contenuto e funzione dell'esenzione*

L'art. 10 del Regolamento delegato (UE) 2018/389 disciplina gli accessi meramente informativi al conto. Il PSP può non applicare la SCA quando il cliente accede direttamente all'home banking soltanto per consultare il saldo o le operazioni eseguite negli ultimi novanta giorni, senza visualizzare dati sensibili relativi ai pagamenti. L'esenzione non opera in occasione del primo accesso e cessa quando sono trascorsi più di centottanta giorni dall'ultima applicazione della SCA.[8]

L'esenzione riguarda esclusivamente l'accesso informativo. Se il cliente decide di effettuare un pagamento, l'operazione dispositiva deve essere autenticata mediante SCA, salvo che ricorra una diversa esenzione prevista dal Regolamento delegato.

La questione affrontata dal Collegio è se il fattore già utilizzato per l'accesso informativo possa concorrere alla SCA del pagamento oppure debba essere nuovamente applicata un'autenticazione completa con due fattori entrambi inseriti nella fase dispositiva.

4.2 *Le Q&A EBA sul riutilizzo*

La Q&A EBA 2018_4141 chiarisce che i due fattori non devono essere necessariamente inseriti nello stesso momento. Un elemento applicato all'accesso può essere riutilizzato per il successivo pagamento, purché venga applicato un secondo elemento quando l'operazione è avviata e la procedura assicuri il dynamic linking con importo e beneficiario.[9]

7 Art. 12, comma 2-bis, del d.lgs. n. 11/2010: salvo il comportamento fraudolento del pagatore, quest'ultimo non sopporta le conseguenze finanziarie se il PSP non ha esigito l'autenticazione forte del cliente.

8 V. supra, nt. 1, per il testo e le condizioni dell'art. 10 del Regolamento delegato (UE) 2018/389.

9 EBA, Single Rulebook Q&A, Question ID 2018_4141, final answer pubblicata il 24 maggio 2019. La risposta chiarisce che gli RTS non fissano un intervallo autonomo per la fornitura dei due elementi nella stessa sessione: uno può essere riutilizzato dall'accesso, purché l'altro sia applicato al pagamento e il dynamic linking sia riferito alla transazione.

La Q&A 2020_5516 estende il principio al caso in cui l'accesso sia avvenuto con un solo fattore beneficiando dell'esenzione dell'art. 10. L'esenzione non viene trasferita al pagamento: il fattore utilizzato per l'accesso continua a concorrere alla procedura e la SCA viene completata con il secondo elemento applicato alla disposizione.[10]

Il passaggio da una funzione informativa a una funzione dispositiva non rende quindi inutilizzabile il fattore già validato; impone di completare l'autenticazione forte con il secondo fattore richiesto per il pagamento.

Ad esempio, nel caso in cui un utente acceda all'app alle ore 10:00 inserendo la password e disponga un bonifico alle ore 10:03, se la sessione è ancora attiva, la password può continuare a rappresentare il fattore di conoscenza. Il PSP deve però applicare al bonifico un secondo fattore di categoria diversa, per esempio un OTP sul dispositivo, e collegare il codice allo specifico importo e beneficiario. Non è necessario chiedere nuovamente la stessa password dopo pochi minuti.

4.3 *Il significato della "medesima sessione"*

La medesima sessione non coincide con la sola vicinanza temporale. Deve esistere una continuità tecnica riconoscibile dai sistemi del PSP: assenza di logout, scadenza, timeout o apertura di un nuovo contesto di autenticazione. La Q&A 2025_7358, relativa a un percorso nel quale il cliente utilizza un prestatore terzo per accedere ai dati e disporre il pagamento, conferma che il riutilizzo presuppone la possibilità tecnica di mantenere la sessione tra le diverse fasi.[11]

Il Regolamento delegato contiene anche una specifica regola di sicurezza: quando viene applicata la SCA per accedere online al conto, il periodo massimo di inattività del pagatore non può superare cinque

10 EBA, Single Rulebook Q&A, Question ID 2020_5516, final answer pubblicata il 15 gennaio 2021. Il riutilizzo è ammesso anche quando l'accesso sia avvenuto con un solo fattore in applicazione dell'esenzione di cui all'art. 10.

11 EBA, Single Rulebook Q&A, Question ID 2025_7358, final answer pubblicata il 3 ottobre 2025. La risposta, riferita a un percorso combinato di account information e payment initiation tramite TPP, condiziona il riutilizzo alla possibilità tecnica di mantenere la sessione attraverso le diverse fasi.

vedi l'articolo online

minuti.[12] Il limite riguarda l'inattività, non la durata complessiva della sessione. Una sessione può quindi proseguire più a lungo se il cliente continua a interagire con il sistema; non può invece restare inutilizzata oltre il limite previsto senza una nuova autenticazione. La Q&A EBA 2018_4068 precisa, inoltre, che la regola opera nei casi in cui è applicata la SCA e non nello stesso modo quando l'accesso beneficia dell'esenzione dell'art. 10.

4.4 *La soluzione del Collegio*

La Decisione n. 4274/2026 aderisce correttamente alla lettura EBA. Il pagamento non beneficia dell'esenzione prevista per la consultazione del conto, ma il fattore già utilizzato per l'accesso può essere riutilizzato nella stessa sessione, purché venga applicato un secondo elemento di categoria diversa e sia assicurato il dynamic linking.

La soluzione supera due orientamenti restrittivi. Il primo riteneva necessario effettuare un nuovo accesso "dispositivo" prima del pagamento. Il secondo escludeva in radice che il fattore utilizzato nell'accesso informativo potesse concorrere alla SCA. Entrambe le letture introducevano un requisito non previsto dal Regolamento delegato e non coerente con le Q&A EBA.[13]

La regola accolta dal Collegio non riduce il livello di sicurezza, perché il pagamento resta comunque soggetto a SCA. Consente però di evitare un passaggio meramente ripetitivo: se il cliente ha già inserito e validato, ad esempio, la password per accedere al conto e la sessione è ancora attiva, non è necessario chiedergli di digitare nuovamente la stessa password pochi istanti dopo. Il fattore di conoscenza già verificato può continuare a essere utilizzato nella medesima sessione, mentre al momento della disposizione viene applicato un secondo elemento di diversa natura, normalmente un OTP o un'approvazione sul dispositivo, collegato allo specifico importo e beneficiario. In tal modo il PSP mantiene intatto il presidio a doppio fattore, ma elimina una duplicazione che non apporterebbe un effettivo incremento di sicurezza e renderebbe il percorso di pagamento inutilmente più lungo e meno fluido.

5. Il CVV dinamico: funzione, classificazione e criticità della soluzione adottata

5.1 *CVV statico e CVV dinamico*

Il CVV (Card Verification Value, indicato anche come CVC o CID a seconda del circuito) è un codice di sicurezza utilizzato soprattutto nei pagamenti a distanza con carta.

Il **CVV statico** è normalmente composto da tre cifre stampate sul retro della carta e rimane invariato. Se viene copiato insieme al PAN e alla data di scadenza, può essere riutilizzato; per questa ragione non costituisce, di regola, un valido fattore SCA.

Il **CVV dinamico** viene invece generato in un'app, in un'area riservata o su uno specifico dispositivo, cambia periodicamente o per singolo utilizzo e ha una durata limitata. La sua funzione è impedire che i soli dati statici della carta siano sufficienti per effettuare un pagamento online.

La maggiore sicurezza del codice non risolve però il problema della classificazione. Per verificare la conformità alla SCA occorre stabilire se il CVV dimostri conoscenza, possesso o inerenza e con quale altro fattore venga combinato.

5.2 *La classificazione indicata dall'EBA*

L'Opinion EBA-Op-2019-06 distingue tre ipotesi. Il codice staticamente stampato sulla carta non costituisce un valido elemento SCA. Il CVV dinamico può invece provare il possesso del dispositivo o dell'ambiente nel quale viene generato. Solo un codice comunicato separatamente all'utente, in modo assimilabile al PIN iniziale di una nuova carta, potrebbe assumere la natura di elemento di conoscenza. La Q&A EBA 2018_4135 formula il punto in termini ancora più netti, affermando espressamente che *"una carta con dynamic card security code può costituire un elemento di possesso, ma il codice non costituisce un*

12 Art. 4, par. 3, lett. d), del Regolamento delegato (UE) 2018/389: quando viene applicata la SCA per l'accesso online al conto, il tempo massimo senza attività del pagatore non può superare cinque minuti. EBA, Q&A 2018_4068, precisa che la regola dei cinque minuti non si applica nello stesso modo quando l'accesso alle informazioni beneficia dell'esenzione dell'art. 10.

13 Per l'orientamento favorevole al riutilizzo v. ABF Roma, 9 luglio 2024, n. 7918 e 2 aprile 2024, n. 3963; ABF Torino, 31 luglio 2024, n. 9093 e 12 settembre 2024, n. 9705. In senso restrittivo, tra le altre, ABF Milano, 20 giugno 2025, n. 5970; 9 aprile 2025, n. 3619; 8 gennaio 2025, n. 93; 10 ottobre 2024, n. 10636; 13 luglio 2024, n. 8155; 1 luglio 2024, n. 7574; ABF Bologna, 6 novembre 2024, n. 11652 e 4 settembre 2024, n. 9591; ABF Bari, 29 maggio 2024, n. 6380.

elemento di conoscenza".[14]

Anche l'OTP ricevuto via SMS è normalmente utilizzato per provare il possesso del telefono o della SIM. Ne deriva che la combinazione tra CVV dinamico e SMS OTP può risultare inidonea se entrambi gli elementi appartengono al possesso. L'Opinion afferma espressamente che SMS OTP e dynamic card security code non assicurano due categorie differenti quando entrambi hanno tale funzione.[15]

La regola non significa che il CVV dinamico sia inutile. Il codice costituisce un presidio antifrode e può concorrere alla procedura di autenticazione. Significa però che la presenza di due codici diversi non dimostra automaticamente l'esistenza di due fattori appartenenti a categorie differenti.

5.3 *I due orientamenti ABF*

Su questo punto si sono formati due orientamenti. Secondo l'indirizzo più rigoroso, occorre classificare autonomamente gli elementi utilizzati nella fase finale del pagamento. Se il cliente inserisce un CVV dinamico e un OTP via SMS ed entrambi provano il possesso, la SCA non è conforme. Questo orientamento è stato seguito, tra le altre, dalle decisioni dei Collegi di Torino n. 7207/2024, Milano nn. 3554/2024, 8153/2024, 3619/2025 e 5970/2025, Palermo nn. 2318/2025 e 2775/2025 e Bologna n. 2856/2025.[16]

L'altro indirizzo considera il procedimento nel suo complesso. Le decisioni favorevoli valorizzano la password o il fattore biometrico utilizzati prima della generazione del CVV e ritengono che tali elementi concorrano alla SCA del successivo pagamento. Su questa linea si collocano, tra le altre, le decisioni dei Collegi di Napoli n. 3006/2025, Torino nn. 5101/2025 e 1709/2025, Bari n. 7097/2025, Palermo n. 7200/2025 e Roma n. 8237/2025.[17]

Il contrasto non riguarda quindi l'utilità tecnica del CVV, ma il criterio con cui deve essere individuata la categoria del fattore: guardando al codice impiegato nella transazione oppure all'intero procedimento attraverso il quale quel codice è stato generato.

5.4 *Il ragionamento della Decisione n. 4274/2026*

Per il pagamento e-commerce di euro 850, la decisione ricostruisce la seguente sequenza: accesso all'area riservata mediante username e password; generazione del CVV dinamico mediante un OTP inviato al dispositivo; inserimento di PAN, data di scadenza e CVV nel pagamento online; conferma dell'operazione mediante un ulteriore OTP.

Il Collegio attribuisce rilievo alla password utilizzata nel procedimento di generazione e ne ricava due conseguenze: la generazione del CVV impiega un elemento di conoscenza e uno di possesso; il CVV risultante può essere qualificato come conoscenza e combinato con l'OTP finale, considerato possesso. È questa seconda conseguenza a rappresentare il passaggio più controverso della motivazione.

La conclusione non appare, infatti, pienamente condivisibile. Considerare il procedimento nel suo complesso è necessario per ricostruire quali fattori siano stati applicati, verificare se uno di essi possa essere riutilizzato nella medesima sessione e accertare se il pagamento remoto sia assistito dal dynamic linking. Da tale valutazione non segue, tuttavia, che il codice generato assuma la categoria del fattore impiegato a monte.

A tal proposito, appare opportuno distinguere:

- il fattore originario, ossia la password, che appartiene alla conoscenza;
- il procedimento di generazione, nel quale possono intervenire password, OTP e controlli tecnici;

14 EBA, Opinion on the elements of strong customer authentication under PSD2, EBA-Op-2019-06, 21 giugno 2019, parr. 25, 28 e 33 e tabelle 2-3; EBA, Single Rulebook Q&A, Question ID 2018_4135, final answer pubblicata il 15 gennaio 2021: «while a card with a dynamic card security code may constitute a possession element, it would not constitute a knowledge element». L'Opinion include il dynamic card security code tra i possibili elementi di possesso, ferma la verifica della specifica implementazione tecnica.

15 EBA-Op-2019-06, par. 44: la combinazione tra SMS OTP e dynamic card security code non soddisfa la SCA quando entrambi gli elementi appartengono alla categoria del possesso.

16 ABF Torino, 19 giugno 2024, n. 7207; ABF Milano, 20 marzo 2024, n. 3554; 13 luglio 2024, n. 8153; 9 aprile 2025, n. 3619; 20 giugno 2025, n. 5970; ABF Palermo, 3 marzo 2025, n. 2318 e 13 marzo 2025, n. 2775; ABF Bologna, 17 marzo 2025, n. 2856.

17 ABF Napoli, 20 marzo 2025, n. 3006; ABF Torino, 27 maggio 2025, n. 5101 e 17 febbraio 2025, n. 1709; ABF Bari, 21 luglio 2025, n. 7097; ABF Palermo, 22 luglio 2025, n. 7200; ABF Roma, 16 settembre 2025, n. 8237.

- il risultato del procedimento, ossia il CVV dinamico successivamente utilizzato nel pagamento.

Il risultato non assume automaticamente la categoria degli elementi impiegati per produrlo[18]. Tale distinzione è coerente con l'approccio funzionale dell'EBA, secondo il quale la classificazione dipende da ciò che l'elemento consente di provare quando viene concretamente utilizzato. Se il CVV dimostra che l'utente controlla il dispositivo o l'ambiente nel quale il codice è generato, la sua funzione resta riconducibile al possesso, anche quando l'accesso sia stato preceduto dall'inserimento di una password.

La criticità emerge con particolare evidenza dal confronto con la Q&A EBA 2018_4135, espressamente richiamata nella decisione, che affronta proprio l'impiego dei dati della carta e dell'SMS OTP quali fattori SCA e afferma che «*while a card with a dynamic card security code may constitute a possession element, it would not constitute a knowledge element*». La risposta non si limita, quindi, a una classificazione generica, ma esclude espressamente che il dynamic card security code costituisca, in quanto tale, un elemento di conoscenza.

Il carattere generale e non vincolante della Q&A non preclude, in astratto, una diversa qualificazione qualora la concreta implementazione tecnica presenti caratteristiche ulteriori rispetto a quelle considerate dall'EBA. Una simile conclusione avrebbe tuttavia richiesto di individuare tali caratteristiche e di spiegare per quale ragione il CVV utilizzato nel caso di specie costituisse «*qualcosa che solo l'utente conosce*», anziché un valore dinamico generato a seguito della verifica di più elementi e collegato al controllo del dispositivo. La sola circostanza che la sua generazione fosse subordinata all'inserimento della password dimostra l'impiego di un fattore di conoscenza nella fase precedente, ma non prova che la credenziale risultante appartenga alla medesima categoria. Fattore utilizzato, procedimento di generazione e codice prodotto restano elementi distinti.

Neppure il richiamo alla Q&A 2018_4141 sembra offrire un fondamento sufficiente alla qualificazione accolta. Tale risposta considera il percorso di autenticazione nel suo sviluppo temporale per stabilire se un fattore già applicato all'accesso possa essere riutilizzato nella medesima sessione e richiede che, al momento dell'iniziazione del pagamento, sia applicato il secondo elemento e sia assicurato il dynamic linking allo specifico importo e beneficiario. In quel contesto, la valutazione complessiva del processo è necessaria per verificare la continuità della sessione, la presenza dei due fattori e il collegamento dell'autenticazione alla singola operazione.

Si tratta, tuttavia, di un problema diverso dalla classificazione del CVV. Il dynamic linking costituisce un requisito aggiuntivo della SCA per i pagamenti elettronici a distanza: assicura che il codice di autenticazione sia specificamente collegato all'importo e al beneficiario, ma non incide sulla distinzione tra conoscenza, possesso e inerenza. Analogamente, la possibilità di riutilizzare un fattore già validato può giustificare la persistente rilevanza della password nella medesima sessione, ma non comporta che la diversa credenziale generata a valle acquisisca la categoria del fattore originario.

La soluzione adottata dal Collegio sembra dunque trasferire al CVV la categoria della password utilizzata a monte, senza spiegare compiutamente perché tale qualificazione debba propagarsi al risultato del procedimento. Il passaggio non trova un supporto diretto nella Q&A 2018_4141 e rimane in tensione con la Q&A 2018_4135, che affronta specificamente la natura del codice di sicurezza dinamico.

Non è in discussione che la sequenza complessiva possa offrire un elevato livello di sicurezza e costituire un efficace presidio antifrode; resta però distinto il problema giuridico della conformità al requisito, previsto dalla PSD2, dell'utilizzo di due elementi indipendenti appartenenti a categorie differenti. La sicurezza complessiva del processo non consente, di per sé, di modificare la qualificazione dei singoli fattori. Sotto questo profilo, la motivazione non scioglie del tutto la tensione con l'impostazione funzionale seguita dall'EBA e richiede cautela prima che il principio enunciato venga esteso a configurazioni tecniche diverse da quella concretamente esaminata.

5.5 *La possibile ricostruzione alternativa e i suoi limiti*

In astratto, la procedura potrebbe essere ricostruita senza qualificare il CVV come conoscenza: la password utilizzata poco prima potrebbe restare il fattore di conoscenza e l'OTP finale il fattore di possesso. Questa alternativa sarebbe coerente con le Q&A sul riutilizzo.

18 Per fare un esempio con una metafora sarebbe come se un visitatore mostrasse un documento di riconoscimento e inserisse un codice personale alla reception; dopo i controlli ricevesse un badge temporaneo. Il badge verrebbe rilasciato a seguito di una verifica dell'identità, ma non diventa per questo esso stesso un documento di identità. Analogamente, il CVV può essere generato dopo la verifica della password senza diventare necessariamente, in sé, qualcosa che "solo l'utente conosce".

Nel caso concreto, tuttavia, non è possibile assumerla come soluzione certa. La motivazione non chiarisce se l'autenticazione effettuata per generare il CVV alle ore 10:23 e la conferma del pagamento alle ore 10:25 appartenessero alla stessa sessione tecnica, né come la sessione dell'app bancaria si collegasse al merchant e all'eventuale ambiente 3-D Secure. La vicinanza temporale non basta, da sola, a dimostrare la continuità della sessione.

6. Q&A e Opinion EBA nella motivazione del Collegio: funzione interpretativa e limiti

Il ruolo attribuito agli atti EBA costituisce uno dei passaggi metodologicamente più delicati della decisione. Tanto nella parte relativa al riutilizzo del fattore di autenticazione quanto in quella dedicata al CVV dinamico, il Collegio ricorre alle Q&A e alle Opinion per definire il significato operativo delle disposizioni sulla SCA. Il richiamo è pienamente comprensibile, considerata la funzione svolta dall'EBA nell'assicurare un'applicazione uniforme della disciplina europea; la motivazione avrebbe tuttavia potuto chiarire con maggiore precisione a quale titolo ciascun atto viene utilizzato e quale sia il limite della sua rilevanza nei rapporti tra PSP e cliente.

Il punto non è che il Collegio ignori la natura non vincolante della soft law. La decisione la riconosce espressamente e precisa che il meccanismo del *comply or explain* riguarda gli orientamenti e le raccomandazioni. Il passaggio rimane però solo parzialmente sviluppato, poiché Q&A, Opinion e Guidelines non sono strumenti tra loro equivalenti. Le Guidelines adottate ai sensi dell'art. 16 del Regolamento (UE) n. 1093/2010 sono soggette al *comply or explain*; le Opinion emanate ai sensi dell'art. 29 sono dirette a favorire la convergenza delle prassi di vigilanza; le Q&A del Single Rulebook, oggi disciplinate dall'art. 16b, forniscono chiarimenti interpretativi, ma non sono vincolanti e non sono assoggettate al regime proprio delle Guidelines.

La distinzione non ha rilievo soltanto classificatorio. Gli obblighi applicabili al PSP devono essere ricavati dalla PSD2, dal d.lgs. n. 11/2010 e dal Regolamento delegato (UE) 2018/389. Q&A e Opinion possono precisare il significato di disposizioni tecniche formulate in termini generali e rappresentano un riferimento autorevole per autorità e operatori, ma non possono introdurre autonomamente obblighi restitutori o regole di responsabilità non desumibili dalle fonti vincolanti.

Questa impostazione emerge con chiarezza nella questione relativa al riutilizzo del fattore. Le Q&A EBA 2018_4141 e 2020_5516 non estendono al pagamento l'esenzione prevista dall'art. 10 del Regolamento delegato per gli accessi meramente informativi al conto. Il pagamento resta soggetto a SCA. Le risposte dell'EBA chiariscono soltanto che il fattore già validato per l'accesso può essere riutilizzato quando l'operazione è avviata nella medesima sessione, purché venga applicato un secondo elemento appartenente a una diversa categoria e sia assicurato il *dynamic linking* all'importo e al beneficiario. Non viene quindi creata una nuova esenzione: si evita la ripetizione di un fattore già verificato e ancora operativo, completando la SCA al momento della disposizione.

Più problematico è l'impiego degli atti EBA nella parte dedicata al CVV dinamico. L'Opinion EBA-Op-2019-06 e la Q&A 2018_4135 classificano il codice in base alla funzione concretamente svolta: il CVV statico non costituisce un valido elemento SCA; il CVV dinamico può integrare un elemento di possesso; un codice comunicato separatamente al cliente può, in determinate circostanze, essere assimilato a un elemento di conoscenza. Il Collegio muove da tali indicazioni, ma qualifica il CVV come conoscenza in ragione della password utilizzata a monte. Proprio perché la Q&A 2018_4135 esclude espressamente tale qualificazione per il *dynamic card security code*, lo scostamento richiedeva l'individuazione di specifiche caratteristiche tecniche idonee a giustificarlo e, come sopra illustrato, il richiamo alla Q&A 2018_4141 non colma questa lacuna.

La questione centrale non riguarda quindi il valore astratto della soft law EBA, ma la coerenza dell'applicazione che il Collegio ne compie: corretta sul riutilizzo del fattore, meno persuasiva sulla riqualificazione del CVV dinamico.

7. Il percorso dell'onere della prova: prova tecnica, SCA e colpa grave

7.1 La prova tecnica dell'operazione

Il PSP deve anzitutto produrre evidenze che consentano di ricostruire il percorso seguito dall'utente e dai sistemi. La documentazione dovrebbe indicare la fase cui ciascun evento si riferisce, il fattore concretamente applicato, la relativa categoria, il dispositivo o il canale utilizzato, l'eventuale continuità della sessione e il dynamic linking.

Non è sufficiente una tabella che riporti l'esito "success" o il generico invio di un OTP. I log devono es-

sere accompagnati da una legenda comprensibile e consentire di distinguere accesso, generazione del CVV, disposizione e conferma. Se una fase rilevante è affidata a un prestatore tecnico, il PSP deve comunque essere in grado di acquisire e produrre le relative evidenze.[19]

La prova deve riguardare anche le azioni preparatorie che possono attribuire al frodatore il controllo dello strumento: reset della password, associazione di un nuovo dispositivo, attivazione di un token o di un wallet, incremento dei massimali e generazione di credenziali dinamiche. La regolarità del pagamento finale non sana un'eventuale carenza nella fase di enrollment o reset.[20]

7.2 *La SCA come prius logico*

La verifica della SCA precede la valutazione della condotta del cliente. Se il prestatore non prova due fattori validi, indipendenti e appartenenti alle categorie richieste, non può trasferire la perdita sull'utente facendo leva sulla sua imprudenza, salvo la frode del pagatore.

Questo ordine logico emerge con chiarezza nelle decisioni che, una volta esclusa o non provata la conformità della SCA, ritengono assorbita la questione della colpa grave.[21] Il principio evita che la condotta del cliente diventi un argomento sostitutivo della prova tecnica che il legislatore pone a carico del PSP.

7.3 *La prova della colpa grave*

Quando la SCA è stata dimostrata, il prestatore deve fornire elementi ulteriori per provare frode, dolo o colpa grave. L'utilizzo corretto delle credenziali non è sufficiente: occorrono circostanze concrete, anche presuntive, relative alle modalità della truffa e al comportamento del cliente.[22]

19 ABF Milano, 22 luglio 2025, n. 7159; ABF Torino, 15 luglio 2025, n. 6952; ABF, Collegio di coordinamento, 11 ottobre 2021, n. 21285. Le evidenze devono essere intellegibili e riferibili alle singole fasi del processo.

20 ABF, Collegio di coordinamento, n. 21285/2021; ABF Torino, 3 luglio 2023, n. 6730; ABF Palermo, 22 luglio 2025, n. 7200, che ha attribuito rilievo autonomo alla mancata prova della SCA nella fase di reset della password.

21 ABF Milano, n. 3619/2025 e n. 5970/2025; ABF Torino, n. 6952/2025. Una volta esclusa o non provata la SCA, la valutazione della colpa grave resta assorbita, salvo la frode del pagatore.

22 ABF, Collegio di coordinamento, n. 22745/2019. Il PSP deve indicare ulteriori circostanze di fatto, relative alle modalità esecutive, dalle quali desumere in via presuntiva la colpa grave.

Nei casi di smishing, vishing o spoofing non esiste una soluzione automatica. L'apparente provenienza del messaggio dalla banca può ridurre la riconoscibilità della frode, soprattutto quando il messaggio si inserisce in un thread autentico o il chiamante conosce dati personali. La valutazione cambia quando l'utente comunica più OTP, ignora messaggi che descrivono chiaramente importo e finalità del codice, modifica password o massimali, installa nuovi dispositivi o esegue trasferimenti verso conti sconosciuti.

Nel caso deciso dal Collegio assumono rilievo cumulativo gli errori presenti nei messaggi, il numero non riferibile alla banca, la comunicazione di più codici, l'assenza di notifiche nell'area riservata e la richiesta manifestamente anomala di eseguire pagamenti per bloccare altri addebiti. Il giudizio di colpa grave non dipende quindi dal solo spoofing iniziale, ma dalla prosecuzione della condotta nonostante una pluralità di segnali di allarme.[23]

7.4 *Gli obblighi organizzativi del PSP*

La conformità della SCA non esclude in assoluto responsabilità per mancato monitoraggio, assenza di alert o gestione inadeguata delle anomalie. Questi profili devono però essere accertati autonomamente e sulla base di specifici obblighi; non possono trasformarsi in una responsabilità oggettiva per ogni frode tecnicamente riuscita.[24]

La distinzione è essenziale. La SCA verifica l'identità o la validità dell'uso dello strumento; il transaction monitoring valuta invece se la transazione presenti caratteristiche anomale rispetto al profilo del cliente, al dispositivo, alla localizzazione o alla sequenza operativa. I due presidi sono complementari, ma rispondono a funzioni diverse.

23 ABF Napoli, n. 3006/2025; ABF Bologna, n. 2856/2025; ABF Torino, 18 marzo 2024, n. 3404. Le decisioni valorizzano, tra l'altro, pluralità degli OTP, messaggi parlanti, durata della frode, modifiche di credenziali e superamento di blocchi o presidi antifrode.

24 Cass. civ., sez. III, 12 febbraio 2024, n. 3780; Cass. civ., sez. I, 13 marzo 2023, n. 7214; App. Milano, sez. I civ., 13 marzo 2026, n. 696. Gli obblighi di sicurezza e monitoraggio devono essere accertati separatamente dal rispetto formale della SCA.

vedi l'articolo online

8. Ricadute operative per i PSP

La pronuncia offre indicazioni immediate per la progettazione dei processi e per la gestione del contenzioso.

8.1 *Documentare la sessione*

Quando il PSP invoca il riutilizzo di un fattore, deve poter dimostrare che accesso e disposizione appartengono alla stessa sessione. I log dovrebbero evidenziare identificativo della sessione, orari, attività, timeout, logout e passaggi tra app, browser, merchant e sistemi di autenticazione. La semplice prossimità temporale non è sufficiente.

8.2 *Separare le fasi del customer journey*

Accesso, generazione del CVV, pagamento e conferma sono fasi distinte. Lo stesso vale per reset della password, enrollment di un nuovo dispositivo e associazione della carta a un wallet. Ogni fase capace di attribuire il controllo dello strumento deve essere autonomamente protetta e documentata.

8.3 *Qualificare i fattori in base alla loro funzione*

Le policy e le difese non dovrebbero limitarsi ad affermare che il CVV dinamico è conoscenza perché generato dopo una password. Occorre descrivere che cosa dimostra il codice, quali fattori intervengono nelle singole fasi, come restano indipendenti e come vengono collegati alla specifica operazione.

Se CVV dinamico e OTP finale sono entrambi ricondotti al possesso, il PSP deve individuare e provare quale distinto elemento di conoscenza o inerenza concorra effettivamente alla SCA. Se si invoca il riutilizzo della password, deve essere dimostrata la continuità tecnica della sessione fino al pagamento.

8.4 *Conservare il contenuto delle comunicazioni*

Il prestatore dovrebbe poter produrre il testo degli SMS o delle notifiche, con indicazione della finalità del codice, dell'importo, del beneficiario o merchant e delle avvertenze di sicurezza. Questi elementi sono rilevanti sia per il dynamic linking sia per l'eventuale prova della colpa grave. L'invio dell'OTP e il suo effettivo inserimento devono essere documentati separatamente.[25]

8.5 *Governare la filiera tecnica*

Nei pagamenti con carta intervengono emittente, merchant, acquirer, circuito, provider 3-D Secure e altri prestatori tecnici. Il PSP che risponde verso il cliente deve organizzare contratti, audit e tempi di conservazione in modo da poter ricostruire l'intero processo. La frammentazione della filiera non può tradursi nell'impossibilità di assolvere l'onere probatorio.

9. La proposta di regolamento sui servizi di pagamento nel mercato interno

Alla data di chiusura del contributo, la proposta di direttiva sui servizi di pagamento e di moneta elettronica e la proposta di regolamento sui servizi di pagamento nel mercato interno non sono ancora definitivamente approvate. L'accordo interistituzionale provvisorio è stato sottoposto alla Commissione ECON il 5 maggio 2026 e il procedimento legislativo è ancora in corso.[26]

Il testo concordato della proposta di regolamento conferma anzitutto la struttura dell'onere probatorio. L'art. 55 mantiene a carico del PSP la prova dell'autorizzazione, della corretta registrazione e dell'assenza di carenze tecniche e precisa che l'autenticazione, anche forte, non è necessariamente sufficiente a dimostrare il consenso, la frode o la colpa grave. Prima di concludere per la responsabilità del cliente, il PSP deve acquisirne la ricostruzione degli eventi.[27]

L'art. 59 introduce una disciplina specifica per le frodi da impersonificazione. Quando un consumatore viene manipolato da un terzo che si presenta come il PSP attraverso canali attribuiti al prestatore e

25 ABF Torino, n. 7207/2024; ABF Napoli, n. 3006/2025. Il contenuto del messaggio può rilevare sia per verificare il collegamento con la transazione sia per valutare se il cliente abbia ignorato indicazioni incompatibili con la ricostruzione del frodatore.

26 Parlamento europeo, Commissione ECON, Provisional agreement resulting from interinstitutional negotiations, PE 787.673 e PE 787.675, 5 maggio 2026. Alla data di chiusura del contributo i testi non risultano ancora definitivamente adottati e pubblicati nella Gazzetta ufficiale dell'Unione europea.

27 Proposta di regolamento del Parlamento europeo e del Consiglio sui servizi di pagamento nel mercato interno, testo concordato PE 787.675, art. 55. La registrazione dell'uso dello strumento e la SCA non sono necessariamente sufficienti a provare autorizzazione, frode o colpa grave; il PSP deve acquisire la ricostruzione dell'utente.

dispone operazioni fraudolente, è previsto il rimborso alle condizioni stabilite dalla norma; la tutela è esclusa in caso di frode o colpa grave del cliente, che devono essere provate dal PSP.[28] La disposizione riconosce quindi una categoria autonoma di frodi nelle quali la vittima può avere materialmente disposto il pagamento sotto inganno.

L'art. 83 rafforza il *transaction monitoring*, imponendo meccanismi destinati a supportare la SCA e a prevenire o rilevare operazioni potenzialmente fraudolente prima dell'esecuzione. L'art. 85 conserva il *dynamic linking* per i pagamenti a distanza e, al par. 12, conferma che i due o più elementi della SCA devono appartenere a categorie differenti. Il testo introduce una deroga circoscritta ai soli elementi di inerenza: il PSP può utilizzare due elementi appartenenti a tale categoria soltanto se dimostra all'autorità competente che la loro indipendenza è pienamente preservata e che la procedura assicura un elevato livello di sicurezza. L'art. 89 demanda all'EBA nuovi RTS su autenticazione, esenzioni, comunicazioni sicure e monitoraggio.[29][30][31]

Il testo provvisorio non generalizza quindi la possibilità di utilizzare due elementi distinti appartenenti alla stessa categoria e non supera il problema affrontato dalla decisione. In particolare, due elementi entrambi riconducibili al possesso continuerebbero a non essere sufficienti. La Decisione n. 4274/2026 manterrà, pertanto, rilievo anche nel nuovo quadro, sia per il riutilizzo dei fattori nella medesima sessione, sia per la corretta classificazione del CVV, da coordinare con i futuri standard tecnici.

28 Proposta di regolamento sui servizi di pagamento nel mercato interno, testo concordato PE 787.675, art. 59. La disposizione disciplina le operazioni fraudolente autorizzate a seguito dell'impersonificazione del PSP, mantenendo l'esclusione in caso di frode o colpa grave del cliente.

29 Proposta di regolamento sui servizi di pagamento nel mercato interno, testo concordato PE 787.675, art. 83. Il transaction monitoring deve supportare la SCA e prevenire o rilevare operazioni potenzialmente fraudolente prima dell'esecuzione.

30 Proposta di regolamento del Parlamento europeo e del Consiglio sui servizi di pagamento nel mercato interno, testo concordato PE 787.675, art. 85, parr. 8 e 12. Il par. 12 conferma che i due o più elementi devono appartenere a categorie differenti e introduce una deroga limitata all'impiego di due elementi di inerenza, subordinata alla piena indipendenza degli elementi e a un elevato livello di sicurezza. Non è prevista una deroga generale per due elementi appartenenti alla categoria del possesso.

31 Proposta di regolamento sui servizi di pagamento nel mercato interno, testo concordato PE 787.675, art. 89. La norma demanda all'EBA nuovi RTS su SCA, esenzioni, comunicazioni sicure, prestatori tecnici e transaction monitoring.

10. Conclusioni

La prima regola enunciata dal Collegio è condivisibile. L'esenzione dell'art. 10 riguarda soltanto l'accesso informativo; il pagamento resta soggetto a SCA. Il fattore già utilizzato per accedere al conto può tuttavia essere riutilizzato nella stessa sessione, purché al momento della disposizione venga applicato un secondo elemento di categoria diversa e sia garantito il dynamic linking. La soluzione è coerente con le Q&A EBA ed evita di imporre la ripetizione di un fattore ancora validamente operativo.

La seconda regola richiede maggiore cautela. Il CVV dinamico è un presidio antifrode e può costituire un elemento di possesso. Non è però automatico che diventi conoscenza perché la password è stata utilizzata nel procedimento di generazione. Il fattore originario, il procedimento e il codice risultante devono essere distinti.

Il richiamo alla necessità di valutare l'intero processo non risolve il problema. Tale approccio non giustifica, senza ulteriori elementi, la trasformazione del CVV da possesso a conoscenza. La qualificazione del CVV costituisce una ratio effettiva della decisione sul pagamento e-commerce, ma il passaggio logico sul quale si fonda rimane in tensione con le indicazioni EBA richiamate dallo stesso Collegio.

Una ricostruzione alternativa, fondata sul riutilizzo diretto della password quale fattore di conoscenza e sull'OTP finale quale fattore di possesso, sarebbe possibile soltanto se fosse dimostrata la continuità tecnica della sessione fino alla conferma del pagamento; tale continuità non emerge con sufficiente chiarezza dalla motivazione pubblicata. La regola operativa è quindi precisa. Quando CVV dinamico e SMS OTP sono entrambi riconducibili al possesso, il PSP dovrebbe quindi individuare e provare quale distinto fattore di conoscenza o inerenza concorra alla SCA della specifica operazione.

Sul piano probatorio, la decisione conferma che la SCA viene prima della colpa grave. Il PSP deve ricostruire il processo con log leggibili, fattori correttamente classificati, evidenza della sessione e dynamic linking. Solo dopo può invocare la condotta gravemente imprudente del cliente. Nel caso concreto, la pluralità dei segnali ignorati rende condivisibile il rigetto del ricorso, ma non riduce l'esigenza di qualificare e provare con precisione il sistema di autenticazione.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it