Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI – DEC. 10614/2022 – PRES. FEDERICO – REL. MIOLA

Strumenti di pagamento – utilizzo fraudolento – inadeguati sistemi di autenticazione – responsabilità dell'intermediario – effetti (d.lgs. n. 11/2010 artt. 7, 8, 10, 10bis, 12).

L'intermediario è responsabile dell'utilizzo fraudolento dei sistemi di pagamento quando non si sia dotato di sistemi di sicurezza compliant con i requisiti della "autenticazione forte" poiché la mancanza, anche parziale, della prova di tale autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. **(MDC)**

FATTO

La ricorrente dichiara di essere titolare di una carta di pagamento emessa dall'intermediario convenuto, tramite la quale veniva effettuato un pagamento *on line* in maniera fraudolenta. Riferisce al riguardo di aver ricevuto da ignoti truffatori un *sms*, pervenuto dal numero ufficiale dell'intermediario, probabilmente al fine di recuperare le credenziali. Gli stessi effettuavano, quindi, un accesso non autorizzato all'applicazione, con conseguente cambio delle credenziali e un successivo pagamento, sottraendole così l'importo di € 780,00.

Insoddisfatta della prodromica interlocuzione avuta con l'intermediario, la ricorrente, citando copiosa giurisprudenza a sostegno, chiede il rimborso della somma fraudolentemente sottrattagli, essendo l'intermediario tenuto a rispondere dei danni conseguenti al non avere impedito a terzi la sottrazione delle sue credenziali di accesso.

Costituitosi, l'intermediario, dopo aver premesso che la controversia attiene all'accertamento del diritto della ricorrente al controvalore di un'operazione *on line*, effettuata in data 28/02/2022, con la carta di cui costei è titolare (n. ****1301), si oppone alle pretese della stessa, rappresentando come dalle verifiche effettuate sia emersa la legittima esecuzione e la sostanziale regolarità della transazione in oggetto.

Le schermate dallo stesso prodotte, infatti, certificherebbero sia che, al momento della materiale esecuzione, i sistemi informativi non hanno rilevato alcuna anomalia o irregolarità, essendo stata l'operazione disposta dietro diretta ed immediata autenticazione da parte della legittima titolare, sia che la stessa è stata eseguita con un sistema dinamico di autenticazione, avendo l'esecuzione richiesto l'utilizzo del codice OTP. A sostegno la resistente riporta, inoltre, specifiche evidenze informatiche attestanti l'avvenuto *enrollment* della carta al sistema autorizzativo di tipo dinamico, funzionante mediante invio con *sms* della *password* dinamica sul numero di cellulare indicato dalla ricorrente nell'atto di denuncia; il fatto che per la transazione in questione la ricorrente risulta essersi regolarmente autenticata in modalità SCA ed ha ricevuto un *sms* con la *password* dinamica; l'avvenuta digitazione manuale del PAN della carta ai fini della relativa esecuzione.

In merito alla ricostruzione dei fatti, l'intermediario sottolinea come sia la ricorrente stessa a dichiarare di aver ricevuto sul proprio telefono un *sms* dal carattere anomalo, contenente un *link* truffaldino, nonché ad ammettere di aver cliccato su detto *link*, inserendo le

credenziali all'interno del sito *"civetta"* così raggiunto. La ricorrente sarebbe stata, quindi, contattata da un finto operatore che chiamava da un numero sconosciuto, dal quale si sarebbe fatta guidare, seguendone pedissequamente le istruzioni. Sembrerebbe dunque palese che la ricorrente, nel corso della procedura, abbia altresì comunicato il codice segreto pervenuto tramite *sms* sul proprio telefono. Tale negligente condotta avrebbe pertanto dato modo al frodatore di porre in essere la transazione contestata.

L'intermediario conclude, pertanto, che la frode in questione sia riconducibile alla tipologia di *phishing* definita *"classica"* nella decisione del Collegio di Coordinamento n. 3498/2012, avendo la ricorrente contribuito in maniera determinante alla compromissione del suo dispositivo di pagamento, fornendo incautamente a terzi i dati che, invece, era tenuta a custodire gelosamente. Parte ricorrente avrebbe potuto, infatti, evitare la truffa utilizzando la diligenza media, posto che l'intermediario, come riferito compiutamente in più campagne informative, di cui è onere della clientela prendere visione, interloquisce con i propri clienti solo tramite canali ufficiali e non richiede mai la comunicazione di dati relativi agli strumenti di pagamento forniti. Nel caso di specie, la frode sembrerebbe essersi perfezionata attraverso il c.d. *sms spoofing* (seguito dalla telefonata del finto operatore, c.d. *vishing*), che consiste nella manipolazione dei dati relativi al mittente di un messaggio, per far sì che esso sembri provenire da numeri o contatti legittimi e che venga raggruppato insieme ad essi. In proposito, l'intermediario richiama copiosa giurisprudenza dell'Arbitro.

Alla luce dell'orientamento consolidato dell'Arbitro (cfr. Collegio di coordinamento n. 5304/2013), infine, l'intermediario ritiene fuor di dubbio che la ricorrente, nel caso in esame, abbia adottato un contegno gravemente colposo, venendo meno agli obblighi a suo carico di diligente custodia dei dati dispositivi. I *log* prodotti dimostrerebbero, infatti, che il sistema predisposto è a più fattori, in linea con gli *standard* esigibili dall'intermediario, in quanto basato sia su codici di accesso statici, sia su una *password* dinamica inviata con *sms* sul numero di cellulare certificato dalla cliente. A tal fine sottolinea che "*la circostanza che l'operazione sia stata compiuta nonostante la presenza di un sistema a due fattori è un indice sufficientemente significativo di una mancanza di diligenza del (…) ricorrente nella gestione degli strumenti atti a preservare la sicurezza delle operazioni*".

In conclusione, l'intermediario chiede il rigetto del ricorso nel merito, stante l'accertata regolarità dell'esecuzione dell'operazione e l'avvenuta corretta autenticazione ed autorizzazione; in via subordinata, nel caso che venga accolta la richiesta di rimborso avanzata dalla ricorrente, chiede la decurtazione della prevista franchigia.

In sede di repliche, la ricorrente, disconoscendo ulteriormente l'operazione fraudolenta posta in essere, richiama gli artt. 10 e 12 del d.lgs. n. 11/2010, alla luce dei quali, nell'ipotesi in cui l'utente neghi di aver autorizzato un'operazione di pagamento, non solo l'intermediario deve provare che l'operazione contestata sia stata autenticata, registrata e contabilizzata (art. 10, comma 1), ma anche che la stessa sia riconducibile sul piano causale ad una condotta dolosa o gravemente colposa dell'utilizzatore (art. 12); con l'importante precisazione che non è consentito inferire la ricorrenza del secondo elemento, il dolo o la colpa grave dell'utente, dalla sussistenza del primo, ossia dalla c.d. regolarità formale dell'operazione (art. 10, comma 2), in coerenza con la *ratio* di fondo della disciplina dei servizi di pagamento, che è quella di istituire un *«regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori»*; cita, altresì, la decisione del Collegio di Coordinamento n. 22745/2019, informata alla c.d. teoria del rischio di impresa, in base alla quale il "*rischio da ignoto tecnologico*" (che si ha quando un'operazione fraudolenta si verifica, benché l'intermediario abbia messo a disposizione della propria clientela i presidi di sicurezza più evoluti) non dovrebbe rimanere a carico degli utenti, vittime delle frodi, ma essere allocato in capo agli intermediari, essendo insito nella loro attività

professionale e, come tale, facilmente amministrabile dagli stessi ad un costo sostenibile; rammenta il principio di diritto con cui il Collegio di coordinamento, nella summenzionata decisione, riconosce che il citato art. 10, comma , «*va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente*»; menziona sul punto l'orientamento della Suprema Corte, secondo cui, tenendo conto *"dei rischi tipici della sfera professionale di riferimento, assumendo come parametro la figura dell'accorto banchiere: spetta pertanto all'intermediario bancario provare di aver adottato tutte le misure idonee a garantire la sicurezza del servizio da eventuali manomissioni"* (Cass. n. 2950/2017; Cass. n. 806/2016); infine, ricorda gli obiettivi del legislatore nazionale e comunitario, fra cui quello di incrementare la fiducia del pubblico negli strumenti di pagamento diversi dal contante, per incentivarne la diffusione, allo scopo ultimo di aiutare la crescita economica, nell'ottica di garantire la sicurezza dei pagamenti elettronici e, al contempo, di agevolare le procedure di rimborso agli utenti in caso di operazione fraudolenta.

In conclusione, la ricorrente rinnova la domanda di rimborso della somma fraudolentemente sottrattagli, senza applicazione della franchigia, oltre al rimborso del contributo di € 20,00 per le spese di procedura. Tanto premesso, si rileva quanto segue in

DIRITTO

La controversia attiene alla richiesta di rimborso di somme indebitamente sottratte a seguito di un operazione fraudolenta compiuta *on line*.

Il ricorso merita di essere accolto.

Preliminarmente, giova rilevare che l'operazione contestata è stata compiuta il 28.02.2022. Pertanto, esse rientrano nell'ambito di applicazione del d.lgs. 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (c.d. PSD), come modificato dal D.Lgs. 218/2017, di recepimento della direttiva 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018.

In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10-*bis* del d. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019).

Come costantemente rilevato da questo Arbitro, la novellata normativa ha rafforzato il regime di speciale protezione e di altrettanto speciale *favor* probatorio a beneficio degli utenti, introdotto dal d. lgs. n. 11/2010 ante modifica e ripetutamente evidenziato da numerose decisioni dell'ABF, anche del Collegio di Coordinamento (cfr. Decisioni n. 991/2014, n. 5304/2014, n. 3498/2012). La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave

dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, comma. 4, d. lgs. n. 11 /2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011

Ai fini che interessano la presente decisione, vengono in considerazione le seguenti principali disposizioni precettive del d. lgs. 11/2010: *a*) l'art.10, comma primo, stabilisce che, in caso di disconoscimento di un'operazione di pagamento da parte dell'utente, è onere del prestatore di servizi di pagamento provare che la stessa operazione è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non si debba a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; *b*) con riguardo a quest'ultimo profilo, l'art. 8 (fatti salvi gli obblighi posti in capo all'utente *ex* art. 7) stabilisce una serie di obblighi gravanti sul prestatore dei servizi, volti a salvaguardare la sicurezza del sistema, primo fra tutti quello di assicurare l'inaccessibilità ai terzi delle credenziali di sicurezza personalizzate; *c*) in difetto della prova della corretta autenticazione, viene meno, per il prestatore dei servizi, la possibilità stessa di riferire le operazioni contestate al cliente; *d*) l'art. 10, comma secondo, precisa che, in ogni caso, l'apparente corretta autenticazione non è, di per sé, necessariamente sufficiente a dimostrare la riconducibilità dell'operazione all'utente che la disconosca, 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'art. 7, essendo, invece, onere del prestatore dei servizi fornire la prova della frode, del dolo o della colpa grave dell'utente; *e*) l'art. 12, comma primo, pone a carico del prestatore di servizi di pagamento le perdite derivanti dall'utilizzo dello strumento smarrito, sottratto o utilizzato indebitamente, intervenuto dopo la comunicazione di smarrimento o furto prevista dall'art. 7, comma primo, lett. *b*); *f*) l'art. 12, terzo comma, nel prevedere la franchigia di € 50,00, entro la quale l'utente può essere tenuto a sopportare la perdita derivante dalle operazioni compiute prima della comunicazione testé menzionata, fa salva l'ipotesi che l'utente «*abbia agito in modo fraudolento o non abbia adempiuto ad uno o più di cui all'art. 7 con dolo o colpa grave*», nel qual caso l'intera perdita resta a suo carico; *g*) l'art. 12, comma 2-*bis* stabilisce, inoltre, che «*salvo il caso in cui abbia gito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente», come definita dall'art. 1, lett. q-bis, necessaria, ai sensi dell'art. 10-bis, quando l'utente accede al suo conto di pagamento on-line, dispone un'operazione di pagamento elettronico ovvero «effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*»; *h*) l'art. 7, comma primo, enuclea gli obblighi gravanti sull'utente abilitato all'utilizzo di uno strumento di pagamento: in particolare, questi è tenuto ad utilizzare detto strumento nel rispetto delle condizioni contrattuali che ne disciplinano l'emissione e l'uso, i cui termini devono essere obiettivi, non discriminatori e proporzionati (comma primo, lett. *a*); il secondo comma precisa, poi, che, «ai fini di cui al comma 1, lettera *a*), l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a proteggere le credenziali di sicurezza personalizzate».

Se ne può dedurre, dunque, alla luce di quanto precede, che la disciplina in parola fa discendere un duplice ed alternativo regime di responsabilità per l'utilizzo non autorizzato di strumenti o servizi di pagamento: il primo, in base al quale, rispetto alle operazioni poste in essere anteriormente alla tempestiva comunicazione al prestatore dei servizi, l'utente è tenuto a sopportare la perdita derivante dall'utilizzo non autorizzato dello strumento o del servizio di pagamento nei limiti della franchigia di euro 50,00, rimanendo il resto a carico del prestatore dei servizi; il secondo, che opera nei soli casi in cui l'utente abbia agito in modo fraudolento o non abbia adempiuto a uno o più degli obblighi di cui all'art. 7 d. lgs. 11/2010 con dolo o colpa grave, in base al quale l'utente assume, invece, una responsabilità piena e, conseguentemente, sopporta integralmente la perdita.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Al riguardo, il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce "*un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta è 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 150 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; in senso conforme: Coll. Coord. decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014. Da ultimo, Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, *ex* art. 10, comma 2, d. lgs. n. 11/2010).

Con specifico riferimento al requisito di autenticazione forte, si aggiunge che ai sensi dell'art. 38 del Regolamento Delegato (UE) 2018/389 della Commissione Europea il requisito di autenticazione forte (SCA) si applica a tutte le transazioni successive al 14/09/2019 e che il Regolamento individua come requisiti ai fini SCA due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza, purché indipendenti tra loro, nonché la presenza di un collegamento dinamico. Inoltre, nella *Opinion* del 21 giugno 2019 (EBA-Op-2019-06) l'EBA ha fornito chiarezza sugli elementi utili alla SCA, con un ulteriore livello di dettaglio, attraverso specifici esempi di soluzioni tecniche, per ciascuna categoria di elementi, *compliant* o meno con le disposizioni regolamentari.

In considerazione della complessità degli adeguamenti, particolarmente rilevanti nel campo dei pagamenti online con carta, e della necessità di un coinvolgimento attivo degli utenti, il 21 giugno 2019 la *European Banking Authority* (EBA) ha riconosciuto alle autorità nazionali la possibilità di concedere ulteriore tempo, rispetto al 14 settembre 2019, per consentire il completamento degli interventi e l'adozione dei nuovi strumenti di autenticazione da parte di tutti i clienti, con esclusivo riferimento alla suddetta categoria di pagamenti. Il 16 ottobre 2019 l'EBA ha pubblicato un parere che indica nel 31 dicembre 2020 il termine ultimo per il completamento degli interventi in tutta Europa. La Banca d'Italia, come autorità competente a livello nazionale, con comunicato stampa del 29 novembre 2019, ha comunicato che si adeguerà alle indicazioni dell'EBA, concedendo a tutti gli operatori che intendano avvalersene una proroga fino a dicembre 2020.

Venendo al caso di specie, dalla denuncia all'Autorità di pubblica sicurezza, acclusa al ricorso, si desume che la ricorrente disconosce un'operazione effettuata *on line*, in data 28/02/2022, alle ore 12:53, dell'importo di € 780,00, realizzatasi mediante invio di un SMS sull'utenza telefonica della stessa, e successivo accesso da parte di costei ad un *link* fasullo,

attraverso il quale fornisce i codici relativi all'operatività dello strumento di pagamento utilizzato.

Alla luce della ricostruzione pacifica dei fatti, essendo la ricorrente convinta della riconducibilità all'intermediario del messaggio *sms* ricevuto, la frode parrebbe inquadrabile in un genere più sofisticato e insidioso del classico *phishing*, del tipo *sms spoofing*. La stessa ricorrente, ammettendo peraltro nella denuncia di aver aperto il *link* ricevuto dai truffatori, allega a sostegno una schermata del messaggio *sms*, asseritamente ricevuto nel giorno della frode, ovvero il 28/02/2022.

Il Collegio rileva sul punto che il messaggio sembrerebbe apparentemente provenire dall'intermediario convenuto, in mancanza di specifiche contestazioni di controparte sul punto, sebbene la data di ricezione non risulti evincibile e non siano stati prodotti i messaggi genuini, precedenti e successivi, tra i quali lo stesso si sarebbe inserito. La chiamata telefonica successiva, invece, risulta provenire da un numero dispositivo mobile privato e non da un numero ufficiale dell'intermediario, potendosi dunque inquadrare la condotta nell'ambito del *vishing*.

A fronte del disconoscimento dell'operazione di pagamento da parte dell'utente, incombe sul prestatore di servizi di pagamento l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi dell'art. 10, commi 1 e 2, del d.lgs. 11/2010.

Nel caso in esame, trova applicazione l'art. 10-*bis*, comma 1, del suddetto d. lgs., come modificato, il quale statuisce che i prestatori di servizi di pagamento applichino l'autenticazione forte del cliente qualora l'utente: *a) acceda al suo conto di pagamento online; b) disponga un'operazione di pagamento elettronico; c) effettui qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.* Il Collegio rileva preliminarmente sul punto che, ai sensi dell'art. 38 del Regolamento Delegato (UE) 2018/389 della Commissione Europea, il requisito di autenticazione forte (SCA) si applica a tutte le transazioni successive al 14/09/2019, e che, ai sensi dell'*Opinion* EBA del 19/10/2019, nonostante la possibile flessibilità negli approcci di vigilanza fino al 31 dicembre 2020, la responsabilità "civile" degli intermediari inadempienti rispetto alla normativa, entrata in vigore il 14.09.2019, rimane ferma. Il Collegio rileva, altresì, che il Regolamento individua come requisiti ai fini della SCA due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza, purché indipendenti tra loro, nonché la presenza di un collegamento dinamico.

Nel caso in esame, l'intermediario ha prodotto evidenze informatiche che dimostrerebbero l'avvenuta regolare esecuzione dell'operazione contestata secondo il protocollo di sicurezza *3DSecure*, come può evincersi, benché non espressamente menzionato nelle controdeduzioni, dalle schermate prodotte. Inoltre, ha fornito evidenze dalle quali risulterebbe la registrazione della carta intestata alla ricorrente al sistema autorizzativo di tipo dinamico, funzionante mediante invio con *sms* della *password* dinamica con codice

OTP al numero di cellulare certificato, la regolare autenticazione dell'utente in modalità SCA, la ricezione di *sms* con la *password* dinamica e l'avventa digitazione manuale del PAN della carta.

Dalle dichiarazioni dell'intermediario, nonché dalle schermate dallo stesso allegate, sembrerebbe trattarsi della digitazione delle credenziali statiche della carta (codice PAN) e dell'inserimento di una *password* dinamica inviata al cliente (OTP).

Con l'*Opinion* del 21 giugno 2019 (EBA-Op-2019-06) l'EBA ha fornito chiarezza sugli elementi utili alla SCA, attraverso specifici esempi di soluzioni tecniche, per ciascuna categoria di elementi, *compliant* o meno con le disposizioni regolamentari. Sul punto, il Collegio rileva che l'autenticazione a mezzo di dati statici della carta e OTP, quanto meno a

far data dal 14 settembre 2019, deve ritenersi non più in linea con gli *standard* richiesti dalla normativa comunitaria, come definiti della opinion EBA. Invero, nel vigore del Regolamento delegato (UE) n. 2018/389, secondo il parere espresso dall'EBA nella citata "*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2"*, mentre l'OTP ricevuto tramite *sms* integrerebbe un elemento di possesso, i dati riportati sulla carta (numero carta di credito, scadenza dello strumento e CVV), non costituirebbero né un elemento di possesso, né un elemento di conoscenza. Orbene questo Collegio, ricollegandosi ai propri precedenti, ed in adesione alle menzionate determinazioni dell'EBA, ritiene che il sistema di identificazione fondata (anche) sui dati presenti sulla carta di pagamento non consenta di rispettare i criteri della identificazione forte, in quanto non idonei a costituire elementi n di conoscenza, né di possesso: "*Diversamente ragionando si incorrerebbe in contraddizione con quanto previsto dall'art. 6 e 7 del Regolamento 389/17, secondo cui gli elementi dell'autenticazione forte del cliente classificati come conoscenza e come possesso non devono essere catturabili o accessibili da soggetti terzi. Il numero della carta e il codice CCV, essendo riportati in chiaro sul fronte e sul retro della carta, sono invece potenzialmente conoscibili e accessibili anche da parte di terzi. Ne deriva che l'unico fattore di autenticazione ad assumere rilievo nel caso di specie è l'invio del codice monouso, utile ai fini della esecuzione delle operazioni contestate* " (Collegio di Napoli, decisione n. 17207/20; decisione n. 8331/2021; decisione n. 3696/2022; Collegio di Roma, decisione n. 11271/20; decisione n. 1643/2022; Collegio di Milano, decisione n. 401/2022). Ne discende che non risulta assolto nel caso di specie, da parte dell'intermediario, l'onere probatorio di corretta autenticazione delle operazioni di pagamento contestate dal cliente, di cui all'art. 10, comma 1 del D.lgs. 11/2010.

E'altresì opinione condivisa del Collegi che, in assenza di un sistema di sicurezza *compliant* con i requisiti dell'autenticazione forte, secondo le posizioni più recenti dei Collegi, il ricorso sia da accogliere integralmente, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente, a meno che non ne sia provata la frode (in senso conforme, tra le altre, Collegio di Napoli, decisioni nn. 17207/2020, 9099/2020; decisione n. 3696/2022; Collegio di Roma, decisioni nn. 9530/2020 e 11271/2020; decisione n. 1643/2022; Collegio di Milano, decisione n. 20840/2019; decisione n. 401/2022; Collegio di Bologna, n. 22586/2020): prova, quest'ultima, che, nel caso in esame, è evidentemente insussistente, non essendo stato fornito dall'intermediario alcun elemento concernente l'eventuale ricorrenza di indicatori di anomalia, come evidenziali dal D.M. n. 112/2007.

Si aggiunga che dalla documentazione prodotta non si ricavano informazioni circa l'attivazione da parte dell'intermediario di un servizio di *SMS Alert*. Il Collegio ritiene di richiamarsi in proposito alla decisione del Collegio di coordinamento n. 8553/2019, a mente della quale "[...] *Fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto*".

L'intermediario richiede, in via subordinata, la decurtazione della "franchigia" di euro 50,00, prevista in contratto. Rileva, tuttavia, il Collegio che la richiesta non può essere accolta, in conformità delle decisioni del Collegio di Coordinamento, in quanto si tratta di un operazione fraudolenta eseguita *on line*, mentre il regime della franchigia, ai sensi dell'art. 12, comma 3, d. lgs. 11/2010, è previsto esclusivamente nelle ipotesi di *"utilizzo indebito dello strumento*

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

di pagamento conseguente al suo furto, smarrimento o appropriazione indebita" (Collegio di Coordinamento, decisioni n. 16237/2018; 24366/2019; 22745/2019).

P.Q.M.

In accoglimento del ricorso, il Collegio accerta il diritto della ricorrente alla restituzione di € 780,00 (….omissis…).