COLLEGIO DI COORDINAMENTO

composto dai signori:

(CO) MAUGERI	Presidente
(CO) LUCCHINI GUASTALLA	Membro designato dalla Banca d'Italia
(CO) SIRENA	Membro designato dalla Banca d'Italia
(CO) DI RIENZO	Membro di designazione rappresentativa degli intermediari
(CO) LAMANDINI	Membro di designazione rappresentativa dei clienti

Relatore: SIRENA PIETRO

Seduta del 20/09/20222

FATTO

I ricorrenti hanno affermato che:
-il 4 ottobre 2021, il Signor M.P., legale rappresentante delle società ricorrenti, avrebbe tentato di effettuare un acquisto *online* mediante lo strumento di pagamento intestato a una di esse, senza riuscirvi;
-avrebbe pertanto contattato l'intermediario resistente, telefonando al numero indicato nel suo sito Internet istituzionale, e un centralino automatico gli avrebbe chiesto di digitare il numero della suddetta carta di credito;
-un sedicente operatore dell'intermediario resistente gli avrebbe poi chiesto alcuni codici nel frattempo ricevuti sul suo telefono cellulare, comunicandogli che l'operazione di pagamento non sarebbe stata comunque eseguita e che la carta di credito di cui si è detto sarebbe stata bloccata per motivi di sicurezza;
-qualche giorno dopo, il Signor M.P. si sarebbe avveduto che le quattro carte di credito in suo possesso (una intestata a lui personalmente e le altre tre alle

società ricorrenti che egli legalmente rappresenta) erano state bloccate e, nel frattempo, erano state utilizzate per eseguire le seguenti operazioni di pagamento *online*: -€ 5.086,00, sulla carta intestata alla società M. s.r.l.; -€ 5.057,60, sulla carta intestata alla società E. s.r.l.; -€ 2.929,00, sulla carta intestata alla società M. s.r.l. (al netto di due operazioni che l'intermediario resistente aveva già provveduto a rimborsare, in quanto il loro importo era superiore a quello del *plafond*); -€ 1.980,00, sulla carta intestata al Signor P.M.;

-tali operazioni non sarebbero state tuttavia autorizzate dai ricorrenti, bensì da un terzo sconosciuto, il quale avrebbe previamente modificato l'utenza telefonica associata alle carte di credito di cui si è detto e, così facendo, le avrebbe poi digitalizzate mediante un proprio dispositivo elettronico (ad es., un telefono cellulare);

-rispetto a tali operazioni, l'intermediario avrebbe omesso di richiedere un'autenticazione forte del cliente (Strong Customer Authentication) per ciascuna delle suddette carte di credito, avendo inviato mediante SMS una sola OTP cumulativa;

-mancherebbe comunque la prova che l'intermediario abbia richiesto un'autenticazione forte del cliente rispetto alle operazioni di pagamento di cui si è detto.

Ciò posto, i ricorrenti hanno domandato che: -l'intermediario resistente sia condannato a restituire gli importi delle operazioni di pagamento disconosciute.

L'intermediario resistente ha affermato che:

-tutte le operazioni contestate dai ricorrenti sarebbero state correttamente contabilizzate, regolarizzate e autenticate mediante l'inserimento delle relative credenziali;

-sussisterebbe la colpa grave del Signor P.M., poiché egli avrebbe comunicato a un terzo malintenzionato i codici necessari per autorizzare l'accesso all'area personale *online* e la variazione della relativa *password* e dell'utenza telefonica associata alle carte di pagamento intestate ai ricorrenti;

-non sarebbe stato riscontrato alcun malfunzionamento dei propri sistemi informatici o intromissione da parte di terzi.

Ciò posto, l'intermediario resistente ha chiesto che: -le domande dei ricorrenti siano respinte, perché infondate in fatto e in diritto.

***

Il Collegio remittente ha ritenuto che:

-sulla base di quanto affermato dal Signor P.M., il suo ricorso dovesse essere considerato come proposto da un non consumatore;

-i ricorsi di cui si è detto dovessero essere riuniti per ragioni di connessione oggettiva;

-l'autenticazione forte del cliente sarebbe richiesta non solo nella fase di esecuzione delle operazioni di pagamento, ma anche in quella di accesso al conto (*login*), di *enrollment* dell'App o di una nuova utenza telefonica, di registrazione della carta su un *wallet*;

-è pacifico tra le parti che, mediante l'inserimento di una OTP, ricevuta mediante SMS sul cellulare del Signor P.M., il 4 ottobre 2021, alle ore 11:10:01, sarebbe stata effettuata la modifica dell'utenza telefonica associata a tutte e quattro le carte di credito in possesso del medesimo, peraltro intestate a soggetti diversi;

-in assenza di precedenti sul punto, sarebbe dubbio che l'invio di una sola OTP, anziché di quattro OTP diverse (ossia, una per ciascuna delle carte di credito di cui si è detto), sia conforme alla normativa che prevede l'autenticazione forte del cliente (SCA) nella fase di modifica dell'utenza telefonica associata a tali strumenti di pagamento;

-le fasi successive (di tokenizzazione delle carte e di autenticazione delle singole operazioni di pagamento) sarebbero state effettuate previo invio di OTP sul nuovo numero di telefono, in uso ai truffatori.

Ciò posto, il Collegio remittente ha riunito i ricorsi e, rilevata la particolare importanza della questione che essi pongono, li ha sottoposti alla decisione di questo Collegio.

DIRITTO

In via preliminare, si deve rilevare che l'art. 10 *bis*, 1° comma, d.lgs. 27 gennaio 2010, n. 11 (*Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE*) statuisce quanto segue: «*Conformemente all'articolo 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente:* […] c) *effettua qualsiasi azione, tramite un canale a*

distanza, che può comportare un rischio di frode nei pagamenti o altri abusi» (sottolineatura aggiunta).

Secondo l'orientamento interpretativo costante di questo Arbitro, la modifica dell'utenza telefonica associata a uno strumento di pagamento rientra tra le azioni che, ai sensi della suddetta disposizione legislativa, possono «*comportare un rischio di frode nei pagamenti o altri abusi*»: essa esige dunque che i prestatori di servizi di pagamento applichino a tal fine l'autenticazione forte del cliente (in tal senso, v., ad es., Collegio di Milano, decisione n. 9222 del 2022; Collegio di Roma, decisione n. 11435 del 2022; Collegio di Bari, n. 11219 del 2022).

***

Ai sensi dell'art. 5, paragrafo 1, del regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017, 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, «*se i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente* […], *l'autenticazione si basa su due o più elementi che sono classificati nelle categorie della conoscenza, del possesso e dell'inerenza e comporta la generazione di un codice di autenticazione. Il codice di autenticazione è accettato solo una volta dal prestatore di servizi di pagamento quando il pagatore lo utilizza per accedere al suo conto di pagamento* online, *disporre un'operazione di pagamento elettronico o effettuare qualsiasi operazione tramite un canale a distanza che possa comportare un rischio di frode nei pagamenti o altri abusi*» (sottolineatura aggiunta).

Nel caso di specie, è pacifico tra le parti che l'accesso (*login*) all'area personale *online* sia avvenuto mediante l'inserimento di una *password*, la quale, ai fini della suddetta disposizione legislativa, rileva come un elemento di conoscenza, idoneo a integrare uno dei fattori richiesti di autenticazione forte del cliente.

Il medesimo elemento di conoscenza è altresì idoneo a costituire il primo dei fattori di autenticazione forte del cliente che sono richiesti per modificare, durante la stessa sessione operativa dell'area personale *online*, la sua utenza telefonica.

Infatti, dando risposta alla Question ID 2018_4141, l'EBA ha precisato quanto segue: «*The Commission Delegated Regulation does not prescribe a time limit for the provision of the two authentication elements necessary for SCA while within a session. When initiating a payment, SCA may therefore be performed when one of*

the elements used at the time the customer accessed its payment account online (including via a mobile app) is reused in compliance with Article 4, and the other element of SCA is carried out at the time the payment is initiated, provided that the dynamic linking element required under Article 97(2) PSD2 and detailed under Article 5 of the Delegated Regulation is present and linked to that latter element» (sottolineatura aggiunta).

***

Per quanto riguarda il secondo dei fattori di autenticazione forte del cliente che sono richiesti per modificare la sua utenza telefonica, si deve premettere che non è stato chiarito dal legislatore europeo se, qualora più strumenti di pagamento siano associati alla stessa utenza telefonica, la modificazione di quest'ultima costituisca un'unica operazione ovvero se si tratti di una pluralità di operazioni distinte. Nel primo caso, l'invio di una sola OTP dovrebbe considerarsi idoneo a costituire uno dei fattori di autenticazione forte (unitamente, ad es., alla *password* statica necessaria per accedere all'App); in caso contrario, occorrerebbe che per ciascuno degli strumenti di pagamento di cui si tratta fosse inviata una OTP diversa.

A tale proposito, si deve rilevare che, dando risposta alla Question ID 2018_4039, la European Banking Authority (EBA) ha affermato che: «*The SMS OTP qualifies as an ownership factor ("something only the user possesses") because it is received on a device that the cardholder owns and that has been securely associated with the cardholder by the issuer*» (sottolineatura aggiunta).

Dando risposta alla Question ID 2019_4560, inoltre, l'EBA ha affermato che: «*In line with the requirements of Article 24 of the Delegated Regulation only a single payment service user can be associated, at a time, with the personalised security credentials, the authentication devices and/or the software*».

Per quanto implicitamente, tali indicazioni dell'EBA depongono nel senso che l'utenza telefonica non sia riferibile a ciascuno strumento di pagamento, bensì a ciascun titolare di uno o più di tali strumenti.

Da ciò discende logicamente che, al fine di modificare l'utenza telefonica associata a più carte di credito, l'invio di una sola OTP mediante SMS ricevuto dal titolare di tale utenza telefonica è sufficiente a integrare uno dei fattori di autenticazione forte del cliente.

La soluzione sopra esposta risulta peraltro coerente con le decisioni fin qui prese dai Collegi territoriali (ad es., v. Collegio di Bologna, n. 10554 del 2022 e Collegio di Bari, n. 23978 del 2021).

***

Al fine di dare sinteticamente una risposta al quesito posto dall'ordinanza di rimessione, questo Collegio enuncia dunque il seguente principio di diritto:

-l'invio di una sola OTP all'utenza telefonica associata a più strumenti di pagamento è idoneo a costituire uno dei fattori di autenticazione forte del cliente che sono richiesti ai fini della modificazione di tale utenza telefonica.

***

Si deve altresì rilevare che l'intermediario resistente ha provato la regolare autenticazione delle singole operazioni di pagamento che sono state disconosciute dai ricorrenti.

PER QUESTI MOTIVI

Il Collegio non accoglie i ricorsi.

IL PRESIDENTE

Firmato digitalmente da
MARIA ROSARIA MAUGERI