Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MIRONE	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro designato dalla Banca d'Italia
(PA) SERIO	Membro di designazione rappresentativa degli intermediari
(PA) VASCELLARO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - ENZO SCANNELLA

Seduta del 16/09/2021

FATTO

Dopo aver invano esperito la fase di reclamo, con ricorso pervenuto in data 03.05.2021, il ricorrente chiede la restituzione della somma di € 4.998,00, corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati.
Il ricorrente è intestatario del contratto di conto corrente ***046, intrattenuto con l'intermediario resistente. In data 26.11.20, recatosi presso uno sportello ATM, il ricorrente si avvedeva della presenza di movimenti sul proprio conto corrente, da lui non effettuati, per complessivi € 4.998,00: più in particolare, il primo addebito ammontava a € 2.898,00 e il secondo a € 2.100,00, entrambi effettuati in data 26.11.20 e disconosciuti nella medesima data. Tali operazioni risultavano estranee al ricorrente, il quale in data 26.11.20 riceveva un sms sul proprio cellulare che lo informava di una anomalia sul proprio conto corrente. Tali operazioni sono state rese possibili grazie all'assenza di sistemi idonei quali sms alert e l'assenza di tecnologia OTP.
L'intermediario, con le controdeduzioni, ricostruita la vicenda - confermando che parte ricorrente contesta la legittimità di due operazioni online - eccepisce che le verifiche effettuate hanno accertato la legittima esecuzione e sostanziale regolarità delle transazioni.
In merito alle modalità di autenticazione delle operazioni, la resistente afferma infatti che le stesse sono state poste in essere all'interno di un sistema dinamico di autenticazione che

ha reso necessario l'utilizzo del Codice ****ID in App. In particolare, alla luce delle evidenze elettroniche, rileva che esse sono state effettuate tramite APP, per la cui installazione e configurazione, è necessario conoscere: le credenziali di accesso ai servizi di internet banking, i dati della carta utilizzata per effettuare i pagamenti online (ossia PAN, CVV2 e data di scadenza) e soprattutto la password dinamica "usa e getta" inviata sul numero di cellulare rilasciato dal cliente a esso intermediario, necessaria per impostare il "codice [nome intermediario] id" per autorizzare le successive disposizioni di pagamento effettuate da app. Sul punto, la resistente richiama i contenuti dell'allegato documento esplicativo "La soluzione xxxId in ottica Strong Customer Authentication" che descrive nel dettaglio il funzionamento di tale sistema.
La responsabilità della frode sarebbe dunque imputabile esclusivamente al cliente, il cui comportamento gravemente colposo ha favorito l'indebito utilizzatore. Invero, come riportato in sede di denuncia e in sede di reclamo, egli ha incautamente cliccato su un link truffaldino, comunicando i propri codici (OTP per l'istallazione dell'APP e creazione di un nuovo xxxID) dando così modo al frodatore di porre in essere la transazione. A sostegno di quanto sopra descritto, riporta specifica evidenza attestante l'avvenuto enrollment della carta nella titolarità del ricorrente al sistema autorizzativo di tipo dinamico funzionante mediante invio della password dinamica tramite sms sul numero di cellulare indicato dal cliente nella denuncia. Chiede quindi al Collegio di respingere il ricorso, atteso che il ricorrente è incorso in una truffa oramai ben nota al pubblico dei consumatori, in merito alla quale esso stesso sta da tempo rendendo edotta la propria clientela. Chiede pertanto il rigetto del ricorso.
In sede di repliche, il ricorrente contesta quanto riferito dall'intermediario in sede di controdeduzioni in merito al servizio di sms alert: in particolare, lo stesso intermediario riconosce che tale sistema "è attivo di DEFAULT sull'APP". Tale circostanza, di fatto, avvalora la tesi in forza del quale nessun alert sarebbe stato ricevuto dal ricorrente, sul proprio numero di cellulare, attesa l'installazione dell'App su diverso dispositivo.
Nessun limite giornaliero di utilizzo, peraltro, è stato previsto dall'intermediario, circostanza che ha consentito al terzo frodatore di effettuare le operazioni contestate. Indice di frode, che avrebbe dovuto determinare il blocco della carta, è rappresentato peraltro dall'installazione dell'APP su un diverso dispositivo, la cui utenza non è associata al ricorrente l'importo oggetto di transazione, inusuale per il ricorrente.
L'operazione, pertanto, è stata resa possibile solo grazie agli scarsi sistemi di sicurezza adottati dall'intermediario, posto il ricorrente non avrebbe mai ceduto a terzi le proprie credenziali di accesso.

DIRITTO

Il ricorso è meritevole di accoglimento per le ragioni di seguito esposte.
Il ricorrente chiede la restituzione della somma corrispondente all'importo di operazioni disconosciute eseguite fraudolentemente da terzi non autorizzati.
Preliminarmente, le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

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 dlgs. 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).
Secondo quanto emerge dagli atti del procedimento, il ricorrente sarebbe stata vittima di un episodio di vishing e smishing, originato da una telefonata e da un sms ricevuti il 26.11.20 (ovvero il giorno stesso del perfezionamento delle operazioni disconosciute). In particolare, in sede di denuncia il ricorrente riferisce di aver ricevuto un sms da un'utenza telefonica privata che termina con******083 (circostanza che consentirebbe di escludere che il ricorrente sia stato vittima di cd. spoofing) con il quale veniva informato della presenza di un'anomalia sul proprio conto corrente e veniva invitato a cliccare su un link; il ricorrente riferisce di aver dato seguito alla richiesta e di aver ricevuto dapprima una chiamata dallo stesso numero e successivamente una chiamata da altra utenza, sempre privata, con la quale veniva invitato a fornire le proprie credenziali e disinstallare l'applicazione presente sulla propria utenza.
Secondo quanto dedotto dall'intermediario, in seconda fase il ricorrente avrebbe comunicato al malfattore le OTP autorizzative così consentendo al terzo di effettuare l'enrollment dell'App su un nuovo dispositivo.
Sulla base delle evidenze prodotte dall'intermediario, il blocco dello strumento sarebbe stato disposto in data 27.11.2020. Non risultano operazioni successive, oggetto di contestazione.
Il ricorrente chiede il rimborso di complessivi € 4.998,00, corrispondente a due operazioni di ricarica online effettuate l'11/02/2021 (comprensive dell'importo di un euro addebitato per ciascuna operazione a titolo di spese).
In base alla tipologia, l'orario e il numero delle operazioni contestate non parrebbe potersi configurare un rischio di frode (cfr. infra, riferimenti normativi, in particolare, D.M. 30 aprile 2007, n. 112) che un efficiente sistema di monitoraggio avrebbe potuto intercettare e valutare al fine di un tempestivo blocco dell'operatività.
Nel caso in esame, le operazioni sono state realizzate tramite digital wallet. Secondo quanto affermato dall'intermediario, l'autenticazione delle operazioni controverse si è articolata in due fasi: configurazione dell'applicazione dell'intermediario su smartphone, con enrollment dello strumento di pagamento; a seguire disposizione delle singole operazioni fraudolente tramite applicazione.
Fase 1: fase preliminare, consistente nella registrazione dello strumento di pagamento nel portafoglio virtuale, il digital (o mobile) wallet.
In primo luogo, occorre verificare se il sistema per l'abbinamento dello strumento di pagamento al digital wallet rispetti i principi dell'autenticazione "forte". A tal proposito, l'EBA, con la Q&A pubblicata il 25/09/2020 (question ID 2019_4910), ha chiarito che l'associazione di una carta di pagamento a un wallet digitale rientra tra quelle azioni che possono comportare un rischio di frode nei pagamenti o altri abusi, di cui all'art. 97 della PSD2, recepito dall'art. 10-bis, primo comma, lett. c) del d.lgs. 11/2010.
L'intermediario descrive il processo di associazione di una carta al wallet in questione. Parte resistente riferisce che per l'associazione della carta al wallet sono state utilizzate le credenziali di accesso ai servizi di internet banking, i dati statici della carta (ossia PAN, CVC2 e data di scadenza), sia la password dinamica "usa e getta" (c.d. OTP: one time password) inviata via SMS sul numero di cellulare appositamente rilasciato dal cliente all'Intermediario) necessario per impostare il codice "***ID" per autorizzare le successive operazioni.

Fase 2: è rappresentata dalle successive autorizzazioni delle transazioni che, in ogni caso, vanno valutate alla stregua dei requisiti prescritti dalla normativa vigente. Secondo il consolidato orientamento dei Collegi in materia (cfr. ex multis, Collegio di Palermo 14147/20) pur in presenza di una corretta installazione del digital wallet con tecnologia a doppio fattore, l'intermediario è tenuto comunque a provare che la doppia autenticazione sia prevista anche al momento della finalizzazione del pagamento.
Nelle operazioni mediante wallet, la SCA è garantita dai seguenti elementi:
-Possesso, integrato mediante la c.d. tokenizzazione della carta sul dispositivo dell'utente. Invero, l'"Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2" riconosce come "compliant with sca" l'utilizzo di una app collegata a un dispositivo mediante la previa registrazione (binding), resa possibile dalla comunicazione dei dati di autenticazione da parte della ricorrente;
-conoscenza ovvero inerenza, a seconda dell'opzione scelta dall'utente (pin, fingerprint, ecc.) rispetto ai metodi supportati dal wallet provider. Tale codice può rilevare sotto il profilo della conoscenza (PIN, Password, memorised swiping path) oppure quale elemento di inerenza, se utilizza i dati biometrici.
Sul punto, l'intermediario afferma che per eseguire le operazioni suddette occorra:
a)il certificato digitale che richiede una password a conoscenza del solo utente-titolare (codice ***ID);
b)una OTP generata in modo random dall'app installata sul proprio device, previo accesso con inserimento delle relative credenziali.

Quanto poi alle modalità tecniche di funzionamento del dispositivo ****ID la resistente svolge inoltre considerazioni tecniche, volte a descrivere nel dettaglio il processo autorizzativo tramite ****ID di una transazione generata da web e autorizzata in App.
Ciò posto, nel caso odierno l'intermediario ha allegato - oltre alla scheda tecnica di funzionamento del xxxid e alla comunicazione rivolta alla clientela che spiega come difendersi dalle truffe – le seguenti schermate: evidenza contabile delle operazioni effettuate; enrollment della carta al sistema autorizzativo di tipo dinamico funzionante mediante invio con OTP al numero di cellulare della cliente corrispondente con quello indicato in sede di denuncia; log dal quale parrebbe evincersi la tracciatura degli sms (inviati al cellulare del ricorrente il 26.11.20 alle 14:08 e alle 14:08) contenenti le OTP dispositive, verosimilmente necessarie per l'enrollment dell'App su nuovo dispositivo e/o per la configurazione del codice ****ID. Il log sopra riportato, peraltro, non chiarisce il contenuto dell'sms inviato.
Il Collegio tuttavia evidenzia che parrebbe mancare evidenza agli atti dei log delle operazioni contestate da cui desumere la sopra descritta modalità autorizzativa. In particolare, l'intermediario non produce videate del proprio sistema informativo da cui possa evincersi la corretta esecuzione, in assenza di messaggi di anomalia, di entrambi i fattori di autenticazione forte richiesti dalla normativa, e, soprattutto, non chiarisce la natura del fattore diverso dall'OTP. Detto secondo fattore, dalle dichiarazioni presentate in sede di controdeduzioni, parrebbe consistere negli elementi riportati sulla plastica della carta.
Al riguardo si osserva che la Opinion dell'EBA del 21 giugno 2019 relativa ai requisiti dei fattori che compongono la strong costumer authentication specifica che i dati stampigliati sulla carta di pagamento non costituiscono un valido elemento riferito al "possesso":
In relazione a quanto precede, per completezza sistematica, si osserva che la Banca d'Italia, nel differire al 1° gennaio 2021 la piena attuazione dei criteri EBA relativi alla cosiddetta autenticazione forte, ha comunque precisato che detto differimento – da richiedere all'Istituto di Vigilanza tramite una apposita istanza di cui nel caso di specie non

v'è presenza in atti – dispiegava i propri effetti unicamente a fini amministrativi e di vigilanza ma NON agli effetti della responsabilità civile (cfr. Comunicazione del 1° agosto 2019).

Ad avviso del Collegio non sussistono i presupposti per ritenere che nella specie detto sistema di autenticazione forte sia stato attuato. Giova ricordare che in base alle determinazioni dell'EBA (Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 del 21 giugno 2019) l'autenticazione forte del cliente «consiste in una procedura basata sull'impiego di due o più dei seguenti elementi - classificati nelle categorie della conoscenza, del possesso e dell'inerenza: i) qualcosa che solo l'utente conosce, per esempio una password statica, un codice, un numero di identificazione personale; ii) qualcosa che solo l'utente possiede, per esempio un token, una smart card, un cellulare; iii) qualcosa che caratterizza l'utente, per esempio una caratteristica biometrica, quale può essere un'impronta digitale. Inoltre, gli elementi selezionati devono essere reciprocamente indipendenti, ossia la violazione di un elemento non compromette l'altro o gli altri. Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione».

Sempre secondo il parere dell'EBA, ai fini dell'autenticazione forte, i dati presenti sulla carta di pagamento non costituiscono elementi né 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. Il ricorso merita, pertanto, di essere accolto, in quanto l'intermediario non ha dimostrato di aver adottato un sistema di autenticazione forte" (Collegio di Napoli, decisione n. 17207 del 5 ottobre 2020).

E' onere dell'intermediario provare:

1.che l'operazione sia stata autenticata, correttamente registrata e contabilizzata (art. 10, D. Lgs. 11/10). In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute (senza applicazione della franchigia): in particolare, l'Arbitro ha ribadito in più occasioni che la mancata prova dell'autenticazione delle operazioni da parte dell'intermediario non consente di prendere in esame i profili afferenti la colpa della ricorrente ai sensi dell'art. 10, comma 2, d.lgs. n. 11/2010;

2.tale prova non è comunque di per sé sufficiente per attribuire le conseguenze patrimoniali della frode al titolare dello strumento di pagamento. L'intermediario, infatti, non si libera dalla responsabilità provando la mera regolarità formale delle transazioni dovendo lo stesso, ai sensi dell'art. 10 del dlgs. 11/2010, fornire altresì la prova, anche in via presuntiva, della colpa grave (o del dolo) dell'utente (cfr. Collegio di Coordinamento – decisione n. 22745 del 10 ottobre 2019).

In questa prospettiva, il Collegio richiamando il proprio orientamento, ritiene che la mancata prova dell'autenticazione dell'operazione da parte dell'intermediario non consenta all'Arbitro di prendere in esame i profili afferenti la colpa della ricorrente ai sensi dell'art. 10, comma 2, d.lgs. n. 11/2010 (Collegio di Bari, decisione n. 24806/18; Collegio di Palermo, decisione n. 4505/2019).

L'applicazione della franchigia, in base al disposto normativo, non è automatica (comma 3 dell'art. 12 del D.lgs. 11/2010 secondo il quale "il pagatore può sopportare, per un importo comunque non superiore a euro 50, la perdita relativa a operazioni di pagamento non autorizzate"). I Collegi territoriali hanno pertanto condiviso l'orientamento per cui la franchigia trova applicazione:
(i) indipendentemente da un'apposita previsione pattizia, salva l'eventuale produzione del contratto da parte del cliente, quale soggetto interessato a far valere le eventuali previsioni più favorevoli sul punto;
(ii) soltanto dietro espressa richiesta dell'intermediario nelle proprie controdeduzioni (anche in virtù del principio della domanda);
(iii) in misura fissa, quale stabilita dalla legge, anche in considerazione delle statuizioni del Collegio di Coordinamento con riguardo alla graduabilità dell'importo della franchigia.
Nel caso in esame non risulta allegata in atti alcuna documentazione contrattuale, né sussiste una contestazione fra le parti in ordine alla disciplina applicabile al rapporto.
Il ricorso è pertanto meritevole di accoglimento. Il Collegio, pertanto, alla luce di tali rilievi, ritiene il resistente tenuto alla restituzione dell'importo complessivo di € 4.998,00 corrispondente alla somma indebitamente sottratta al ricorrente.

PER QUESTI MOTIVI

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 4.998,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARIA ROSARIA MAUGERI