COLLEGIO DI BARI – DEC. N. 17120/2020 – PRES. TUCCI - REL. RUSSO

Strumenti di pagamento – indebito utilizzo – standard di sicurezza – inosservanza - responsabilità dell'intermediario (d.lgs n. 11/2010 art. 10)

L'intermediario risponde dell'indebito utilizzo di uno strumento di pagamento quando non si sia dotato di sistemi di sicurezza adeguati agli standard in uso. **(MDC)**

FATTO

Il ricorrente, titolare di una carta di debito emessa dall'intermediario resistente, riferisce di aver risposto ad un sms che richiedeva l'inserimento di nome utente e password; successivamente, cliccando sull'apposito link ricevuto, veniva reindirizzato sulla pagina web dell'intermediario, ove procedeva ad inserire i codici di accesso. Afferma di aver poi ricevuto un messaggio di "*richiesta di abilitazione a G***** Pay*" contenente un codice di verifica. Fa presente che, il giorno successivo, constatava l'avvenuto prelievo di € 1.170,00 sulla propria carta, effettuato da un soggetto terzo, a lui ignoto.

Procedeva pertanto a sporgere denuncia e ad inoltrare modulo di contestazione.

Chiede, pertanto, il rimborso della somma indebitamente sottratta, pari ad € 1.170,00.

Costituitosi, l'intermediario rappresenta che, dalle verifiche effettuate, è emersa la legittima esecuzione e la sostanziale regolarità della transazione contestata, essendo stata disposta dietro diretta ed immediata autenticazione da parte del legittimo titolare.

Precisa, altresì, che l'operazione di pagamento in questione è stata eseguita mediante l'ausilio del Token, per il tramite dell'applicazione mobile G***** Pay, che prevede l'inserimento dei dati della carta, nonché di una password dinamica "usa e getta" (c.d. OTP) inviata al numero di cellulare del cliente.

Fornisce a tal proposito, tracciatura del SMS con OTP ricevuto dal numero di cellulare del cliente, necessario ai fini dell'installazione e della configurazione dell'App, secondo un c.d. sistema di autenticazione "a due fattori". Allega inoltre specifica evidenza attestante l'avvenuto *enrollment* della carta di pagamento del ricorrente al sistema autorizzativo di tipo dinamico.

Ritiene sussistente la colpa grave del ricorrente, sottolineando che i log prodotti dimostrano che il sistema predisposto è a più fattori, in quanto basato sia su codici di accesso statici sia su una password dinamica inviata con sms sul numero di telefono cellulare certificato dal cliente. Ravvisa una violazione degli obblighi di diligente custodia dello strumento di pagamento da parte del cliente, avendo egli per sua stessa ammissione, resa nel verbale di denuncia, cliccato su un link truffaldino ed inserito tutti i dati relativi alla propria carta, oltre alla password dinamica. Sottolinea come tale truffa, ormai nota, possa essere evitata usando una diligenza media.

Richiama infine alcune pronunce dell'Arbitro (Collegio di Milano n. 18113/2019, n. 4380/2012 e n. 2081/2013), secondo cui "*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*".

Conclude per il rigetto del ricorso; nella denegata ipotesi di accoglimento della richiesta di rimborso, chiede, la decurtazione della prevista franchigia.

DIRITTO

L'operazione contestata è stata eseguita 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 13/1/2018.

In particolare, l'articolo 10, commi 1 e 2, del citato decreto dispone che "*Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo della colpa grave dell'utente*".

In una recente pronuncia, il Collegio di Coordinamento, dopo aver osservato che "*l'onere probatorio previsto nei commi 1 e 2 dell'art.10 del decreto deve necessariamente essere assolto dal PSP con riguardo ad ambedue i profili (autenticazione ed esecuzione delle operazioni di pagamento, nonché colpa grave dell'utilizzatore), da ritenersi necessari e complementari",* ha enunciato il seguente principio di diritto: "*[…] la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, 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*" (Coll. Coord., dec. n. 22745/2019).

Ora, venendo al merito del ricorso, il Collegio rileva che, Il ricorrente in sede di ricorso afferma di aver ricevuto un sms e di aver cliccato sul link ivi contenuto, venendo così reindirizzato su una pagina web intestata all'intermediario, ove inseriva i codici di accesso.

L'operazione contestata consiste in un prelievo di € 1.170,00, disposto in data 18/02/20 alle ore 22:48, come si evince dal modulo di disconoscimento e dalla schermata prodotta dall'intermediario.

In merito all'adeguatezza dei presidi predisposti dall'intermediario, si rileva che le operazioni contestate sono state effettuate tramite il sistema di pagamento G*** Pay. In base a tale sistema, secondo quanto si desume dalla descrizione fornita dalla resistente, sarebbe necessario un codice OTP soltanto per l'installazione iniziale dell'app, mentre le successive operazioni verrebbero disposte, apparentemente senza necessità dell'OTP, mediante la suddetta piattaforma. L'intermediario produce altresì la documentazione riguardante l'invio del predetto codice OTP per l'attivazione dell'app e dell'esecuzione dell'*enrollment* della carta di pagamento al sistema autorizzativo di tipo dinamico. L'intermediario non ha dunque provato specificamente di avere adottato un sistema di sicurezza c.d. "a due fattori", che preveda per l'esecuzione della disposizione di pagamento, oltre all'inserimento delle credenziali statiche della carta, l'utilizzo di una password dinamica (OTP) ricevuta su un dispositivo mobile esclusivamente in possesso del cliente. Per quanto detto, infatti, sembrerebbe sufficiente per il truffatore conoscere le credenziali (statiche) del cliente per accedere al Portale dell'intermediario (nonché i dati, sempre statici, del cliente e della carta), per poi scaricare l'APP e ricevere o visualizzare l'OTP per attivare G*** Pay ed effettuare il pagamento tramite *contactless*. In altri termini, è necessaria una password OTP per installare l'App su di un dispositivo, ma non anche per autorizzare le singole operazioni di pagamento (cfr., per un caso analogo, Coll. Bologna, n. 4318/ 2019). Ne consegue che si deve presumere che il sistema di sicurezza predisposto dall'intermediario per l'utilizzo della carta virtuale in questione sia a un solo fattore, in più occasioni ritenuto non adeguato dal Collegio rispetto gli standard tecnici in uso. Va pertanto accolta la domanda di parte ricorrente in merito all'utilizzo fraudolento dello strumento di pagamento. Pertanto, la domanda di rimborso del complessivo importo delle operazioni contestate merita accoglimento. (in tal senso, Coll. Bari, dec. n. 11729/2020).

Dalla documentazione prodotta non si ricavano informazioni circa l'attivazione del servizio di SMS alert, né le parti riferiscono alcunché. Si tratta, ad ogni buon conto, di un elemento privo di rilievo ai fini della decisione, atteso che nella specie è stata posta in essere una sola operazione.

Si osserva, infine, che non può essere accolta la richiesta, formulata dall'intermediario in via subordinata, di applicazione della c.d. "franchigia", in quanto la stessa è prevista in ipotesi di "utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita." (art. 12, co. 3 d.lgs. n.11/2010)", laddove, nel caso di specie, l'operazione fraudolenta contestata è una transazione *on line*.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 1.170,00 (…omissis…).