COLLEGIO DI COORDINAMENTO – DEC. 8672/2024 – PRES. MAUGERI – REL. CARRIERO

Strumenti di pagamento- asserita clonazione - esclusione – sms alert - mancata attivazione – effetti (cod.civ., art. 1176; d.lgs. n. 11/2010 artt.7, 8 e 10).

***"Anche nel caso in cui venga esclusa la clonazione dello strumento di pagamento, la mancata prova dell'attivazione del servizio di sms – alert da parte dell'intermediario rappresenta una violazione al corretto adempimento degli obblighi posti a suo carico"* (MDC)**

FATTO

1. Afferma la ricorrente che, avendo in data 11 luglio 2023 fatto accesso a uno sportello ATM per effettuare con la propria carta di debito un prelievo di € 200,00 l'operazione non sarebbe andata a buon fine a causa di "fondi insufficienti", essendo riuscita a prelevare soli € 70,00. Dal conseguente controllo del proprio estratto conto avrebbe accertato l'esistenza (a sua totale insaputa e senza il suo consenso) di 5 prelievi per complessivi € 1.300,00 realizzati tra il 5 e il 29 giugno 2023. Effettuata immediata denuncia presso le competenti autorità pubbliche con espresso disconoscimento delle riferite operazioni imputate a terzi ignoti a seguito di possibile clonazione della carta, rappresentava nella stessa giornata l'occorso all'intermediario bloccando la carta lo stesso 11 luglio 2023 e, dichiarato l'esclusivo possesso tanto della carta quanto dei relativi codici di accesso ai servizi on line, chiedeva il rimborso delle operazioni disconosciute. A seguito del diniego e della inutile proposizione del prodromico reclamo, reitera col ricorso la domanda di rimborso dell'importo di € 1.300,00, oltre agli interessi legali. Si riserva la successiva determinazione e quantificazione dei danni.
2. Costituitasi, parte resistente eccepisce che, riguardando la denuncia soltanto l'addebito illecito e non anche il furto o lo smarrimento del dispositivo utilizzato, si può dedurre che la carta di debito in questione sia sempre rimasta nella disponibilità della legittima titolare. La sola possibilità di eseguire operazioni fraudolente consisterebbe pertanto nella clonazione dello strumento di pagamento. E tuttavia tale circostanza sembra dover essere esclusa in quanto le operazioni risultano correttamente contabilizzate, registrate, autenticate e poste in essere con il corretto inserimento delle credenziali personali della cliente. Ciò risulterebbe altresì avvalorato dal rilievo che non è usuale per un frodatore l'impiego della carta asseritamente contraffatta per effettuare operazioni saltuarie con importi inferiori al massimale consentito, per un verso; dal fatto che le operazioni siano avvenute nella zona di domicilio della ricorrente, laddove tale circostanza normalmente non si verificherebbe nel caso di effettiva clonazione, ove l'utilizzo avverrebbe addirittura all'estero e, in particolare, in Paesi che utilizzano ancora ATM di vecchia generazione, per altro verso. Conclude per il rigetto del ricorso.
3. Seguono repliche e controrepliche con le quali le parti reiterano le rispettive domande. La ricorrente, in particolare, insiste per la clonazione della propria carta di debito.
4. Richiamato, in limine, il particolare regime di ripartizione dell'onere probatorio disciplinato dall'art. 10 del vigente d. lgs n. 11/2010 (e successive modificazioni e integrazioni) a carico del prestatore di servizi di pagamento tanto in punto di corretta

autenticazione delle operazioni disconosciute quanto di uso indebito del dispositivo imputabile all'utilizzatore in violazione degli obblighi di condotta di cui all'art. 7 del riferito testo normativo, si osserva dal Collegio remittente che l'intermediario ha fornito piena prova (sul piano generale come sul concreto versante della fattispecie in rassegna) dell'autenticazione delle operazioni di pagamento ex art. 10 cit., essendo (tra l'altro) la carta dotata della c.d. tecnologia a "micro – chip". Né, sotto il lamentato versante da parte della ricorrente della probabile clonazione da parte di terzi dello strumento di pagamento, ricorrono elementi descrittivi, induttivi o anche solo circostanziali utili a prefigurarne una (sia pure astratta) verosimiglianza. Per contro, osserva il remittente che l'intermediario ha documentato "varie circostanze che rendono plausibile dedurre che lo strumento di pagamento…non sia stato clonato, dovendosi così presumere che esso sia stato utilizzato, all'insaputa della ricorrente, da terzi che hanno potuto disporre, anche solo temporalmente, della carta". Donde una possibile violazione da parte della stessa delle condotte ex art. 7 cit. nella parte in cui prescrivono l'obbligo del titolare di "utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso", nonché di adottare "misure idonee a garantire la sicurezza".
5. Dalla documentazione in atti non risulta tuttavia l'attivazione del servizio di sms – alert da parte dell'intermediario che, ove adottato, ben avrebbe potuto prevenire il compimento delle operazioni indebite successive alla prima (per l'importo di 200,00 euro), limitando la perdita della ricorrente a questa sola operazione di prelievo. Ricordati il rigoroso orientamento di questo Collegio di coordinamento in ordine alla doverosa attivazione di siffatto servizio di protezione dell'utente [ex art. 8, lett c) d. lgs. cit.], la cui mancanza costituisce "una carenza organizzativa" imputabile all'intermediario il quale "non dovrebbe limitarsi a proporlo al cliente ma adottarlo in modo generalizzato a prescindere dal fatto che il cliente ne abbia o meno richiesto l'attivazione" (Coll. coord., n. 24366/19) e i conformi orientamenti dei Collegi territoriali sul punto, il remittente solleva la questione della rilevanza da riconoscere alla mancata attivazione dei messaggi alert in caso di non provata clonazione dello strumento di pagamento a fronte di una ipotizzabile "condotta gravemente negligente della ricorrente nella custodia dello strumento e delle relative credenziali", aggravata dal ritardo nella verifica dell'esecuzione delle operazioni disconosciute.

DIRITTO

6. E' appena il caso di premettere che all'obbligo dell'utente di "comunicare senza indugio" al prestatore di servizi di pagamento (per ciò che qui rileva) "l'uso non autorizzato dello strumento non appena ne viene a conoscenza" [art. 7, lett. b), d. lgs cit.] è correlato – in capo all'intermediario nei pagamenti – il corrispondente obbligo di "assicurare che siano sempre disponibili strumenti adeguati affinché l'utente possa eseguire" la riferita comunicazione [art. 8, lett. c), Id.]. Come già questo "coordinamento" ha avuto modo di stabilire, ben può/deve ritenersi che "l'attivazione dello strumento di segnalazione sms - alert rientri nei su menzionati doveri di adottare misure idonee a garantire la sicurezza del servizio con la dovuta diligenza" (Coll. coord., cit.). Ciò anche sulla scorta degli univoci orientamenti della S.C. di Cassazione i quali, ancor prima del recepimento della disciplina europea, in materia erano nel senso che "non può essere omessa" (ai fini del giudizio di responsabilità dell'intermediario) "la verifica dell'adozione delle misure idonee a garantire la sicurezza del servizio", avendo la diligenza posta a carico del professionista "natura tecnica che deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento" a norma dell'art. 1176, co. 2, cod. civ. (v. Cass., n. 13777/2007). A fortiori, siffatta scelta di allocare in capo al fornitore dei servizi di pagamento questo costo organizzativo che, insieme agli ulteriori, indefettibili presidi tecnologici di sicurezza rappresenta un concreto parametro della diligenza dovuta nello svolgimento di una attività non priva di rischi, trova ancora più puntuale conferma nella giurisprudenza più recente

(v., tra le altre, oltre a Cass. n. 2950/2017 menzionata dal ridetto “coordinamento”, Id., nn. 9158/2018; 18045/2019; 26916/2020 e, da ultimo, n. 3780/2024) la quale espressamente sussume tali rischi nel paradigma più generale del rischio d’impresa, destinato a essere fronteggiato solo attraverso l’adozione di misure che consentano di verificare se l’operazione sia effettivamente attribuibile al cliente, anche attraverso il servizio di sms – alert; misure che “se non azzerano, di certo concorrono a diminuire in modo rilevante questi fenomeni truffaldini” (App. Firenze, n. 1945/22). A ciò consegue (come d’altronde rilevato anche dal Collegio remittente) che la mancata attivazione del servizio sms – alert costituisce in ogni caso una carenza organizzativa imputabile all’intermediario che, oltre a produrre l’effetto giustificativo solo a fronte della specifica dichiarazione liberatoria di rifiuto del cliente ad avvalersene (già affermata dal precedente “coordinamento”), non può non essere rilevata anche d’ufficio. Vale, sul punto, peraltro avvertire (diversamente da quanto ritenuto dal Collegio remittente in ordine alla asserita mancata contestazione da parte della ricorrente dell’assenza di questo strumento) che dalla documentazione in atti consta, per contro, l’espressa sua lagnanza in ordine alla mancanza di comunicazioni della specie (sulla circostanza che il servizio di sms – alert costituisce uno standard di sicurezza normalmente esigibile, la cui assenza configura un’ipotesi di responsabilità da inadeguata organizzazione dell’intermediario, v. anche Coll. coord., n. 16237/2018. In termini gli orientamenti dei Collegi territoriali. V., ad es., tra le più recenti, le decisioni dei Collegi di Milano, n. 2708/2024 e Palermo, n. 4535/2024. A ciò segue la rilevabilità d’ufficio del mancato inoltro degli sms – alert; in termini, tra le tante, Collegio di Palermo, n. 4535/2024; Bologna, n. 21634/2019; Bari, n. 10735/2023; Roma, n. 4370/2021).
7. Peraltro, sul piano della diligenza dovuta dalle parti nel caso di specie è, dal lato dell’intermediario, per tabulas oggettiva la riferita carenza probatoria in ordine al dovuto sistema di alert; da quello del cliente (oltre alla analoga carenza dell’onere probatorio dell’asserita clonazione, riguardo alla quale non vengono offerti neanche elementi circostanziali) la circostanza che sia la carta che le relative credenziali siano rimaste nella dichiarata sua disponibilità e controllo vale a legittimare il ragionevole dubbio del Collegio remittente “che le operazioni di pagamento siano state effettuate, all’insaputa della ricorrente da soggetti… (familiari, collaboratori domestici etc.) che abbiano avuto facile accesso allo strumento di pagamento e alle relative credenziali” anche in ragione del fatto che le operazioni sono avvenute nella zona di domicilio della ricorrente. Ciò che appare idoneo a radicare un ragionevole giudizio di colpevole sua violazione delle richiamate regole di condotta nella custodia dello strumento di pagamento e delle credenziali. Per altro verso, invece nessun significativo ritardo nella verifica delle operazioni indebite appare (nell’ambito della diligenza esigibile) in concreto imputabile alla ricorrente, la quale ha anzi tempestivamente denunciato all’intermediario la circostanza lo stesso 11 luglio 2023, a seguito del prodromico, pressoché contestuale controllo dell’estratto conto avvenuto proprio a seguito dell’accesso all’ATM che ha evidenziato le menzionate irregolarità. Condotta che lascia ragionevolmente presumere che, ove attivato, il servizio sms – alert, ben avrebbe potuto (in ragione della scansione temporale dei prelievi) evitare l’esecuzione delle operazioni indebite successive alla prima, che le va comunque addebitata. Perdita patrimoniale codesta che, a ben vedere, rappresenta più in generale per l’utente dei servizi di pagamento il legittimo, dovuto costo proprio dell’eventuale difetto di custodia della carta e delle credenziali nell’ambito delle operazioni on line (riferibile alla prima o, *ratione temporis*, alle prime operazioni) senza doversi necessariamente estendere all’intera attività truffaldina quando il cliente disponga del e impieghi diligentemente le risultanze del riferito servizio di alert.
8. Pertanto, considerata la natura di carattere organizzativo del servizio di sms – alert tesa a garantire la sicurezza dell’attività dei pagamenti; rilevato che, nel caso di specie, le cinque operazioni disconosciute dalla ricorrente sono state eseguite nell’arco temporale

compreso tra il 5 e il 29 giugno 2023; accertato che quelle successive alla prima risalgono al 22 giugno dello stesso anno; valutato che la perdita relativa alla prima operazione (dell'importo di 200,00 euro), resta comunque a carico della ricorrente a fronte della ricordata esclusione di ogni prova della clonazione della carta e della sua ragionevolmente presumibile colpevole condotta, da un lato, del rilievo che il servizio di alert non ne avrebbe potuto evitare il compimento, dall'altro; ritenuto che l'attivazione del servizio sarebbe invece stata utile, attraverso il blocco della carta, a prevenire le successive, questo Collegio accerta il diritto della ricorrente alla restituzione da parte dell'intermediario dell'importo di complessivi 1.100,00 euro oltre interessi legali dalla data del reclamo.
9. Quanto sopra conduce al seguente principio di diritto:
"Anche nel caso in cui venga esclusa la clonazione dello strumento di pagamento, la mancata prova dell'attivazione del servizio di sms – alert da parte dell'intermediario rappresenta una violazione al corretto adempimento degli obblighi posti a suo carico".

P. Q. M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto della ricorrente alla restituzione dell'importo di 1.100,00 euro oltre agli interessi legali dalla data del reclamo (…omissis…).