COLLEGIO DI PALERMO – DEC. N. 8326/2017 – PRES. MAUGERI – REL. CIRAOLO

Strumenti di pagamento – utilizzo fraudolento – responsabilità - concorso di colpa - fattispecie (cod. civ., art.1176; d.lgs. n. 11/2010, artt.7 e 12)

FATTO

La ricorrente afferma di avere effettuato, nel mese di novembre 2016, un controllo sul proprio conto corrente, allertata dal ricevimento di un sms sul cellulare del proprio coniuge, con il quale questi veniva avvisato di un tentativo di pagamento non autorizzato con carta di credito. Da tale controllo emergeva che tra il 13/10/2016 e il 4/11/16 erano state eseguite diverse operazioni di pagamento non autorizzate con due carte di credito alla stessa intestate, per un importo di € 5.482,12, quanto alla carta "Blu Mastercard n. ***09", e di € 11,90, quanto alla carta prepagata "Superflash Paypass n. ***14".
Dopo avere denunciato il fatto alla Questura di Sassari in data 19/11/2016, la ricorrente integrava l'originaria denuncia il 21/11/2016, specificando di aver individuato nella propria collaboratrice domestica la responsabile delle operazioni fraudolente.
Il 22/11/2016 provvedeva inoltre al disconoscimento delle suddette operazioni presso la filiale dell'intermediario ove intratteneva il proprio conto corrente, chiedendo la restituzione delle somme addebitate. Riferisce tuttavia che l'odierna resistente, dopo avere provveduto a riaccreditare provvisoriamente gli importi relativi alle transazioni contestate, rigettava la richiesta di rimborso dei movimenti posti in essere con la carta Mastercard (salvo che per l'importo di € 2,52), in quanto eseguiti su siti internet certificati sicuri, tramite utilizzo dei codici associati alla carta e senza clonazione della medesima (venivano invece stornati i movimenti eseguiti con la carta Superflash, pari a complessivi € 11,90, con invito a rivolgersi alla filiale per il recupero del saldo della carta).
Contestando la mancata adozione, da parte dell'intermediario, degli accorgimenti necessari ad evitare azioni illecite di terzi (posto che lo strumento in questione non disponeva di un codice PIN identificativo del titolare e che non era stato attivato dalla resistente il servizio di *sms alert*) e ritenendo che nessun rimprovero di negligenza possa esserle mosso (avendo sempre custodito con cura lo strumento di pagamento ed essendosi prontamente attivata al primo sospetto di attività illecita), la ricorrente chiede il riaccredito dell'importo di complessivi € 5.493,02, oltre al pagamento delle spese di procedura.
La banca resistente precisa che la somma di cui la ricorrente chiede il rimborso non tiene conto dell'importo di € 4.964,70, recuperato tramite circuiti internazionali e riaccreditato alla cliente a seguito del deposito del ricorso, in data 03/04/2017 (con conseguente riduzione del credito residuo ad € 514,90, corrispondente all'unica operazione disconosciuta non recuperata). Rileva inoltre che l'invito a presentarsi presso la filiale di Sassari per il recupero del saldo della carta prepagata Superflash è rimasto disatteso dalla cliente.
Ancora, eccepisce che la richiesta di rimborso avanzata nei propri confronti sarebbe illegittima, in quanto andrebbe indirizzata direttamente all'autrice del furto (persona nota alla ricorrente, che avrebbe peraltro ammesso le proprie responsabilità), anche al fine di evitare l'eventualità di un duplice rimborso per i medesimi fatti.
Sotto il profilo tecnico, precisa che la tracciatura delle operazioni contestate dimostra che

esse sono state sempre effettuate su siti di "*commercio elettronico non sicuro*" (ovvero su siti dove, per perfezionare l'acquisto, è sufficiente inserire i dati riportati sulla carta), ad eccezione dell'operazione di € 514,90, eseguita invece su un sito di "*commercio elettronico sicuro*", che richiede l'inserimento di un'apposita *password* (SecureCode MC), evidentemente carpita alla cliente insieme alla carta. L'utilizzo fraudolento, pertanto, sarebbe dipeso esclusivamente dall'inosservanza degli obblighi di custodia delle carte e delle relative credenziali da parte della titolare, non potendo ritenersi responsabile l'intermediario per operazioni eseguite con la digitazione di dati noti soltanto alla cliente.
Il comportamento negligente della ricorrente, inoltre, sarebbe avvalorato dal fatto che costei si è accorta delle operazioni contestate dopo oltre un mese dalla prima transazione non autorizzata, laddove un blocco tempestivo dello strumento avrebbe certamente evitato il perpetrarsi degli abusi. Per di più, diverse circostanze di fatto indicate nella denuncia del 19/11/2016 (mancanza di piccole somme di denaro nella propria abitazione, nonché insistenti richieste di denaro avanzate dalla domestica per far fronte ad alcuni debiti), avrebbero dovuto suggerire alla ricorrente una più attenta gestione del proprio strumento di pagamento.
L'intermediario, pertanto, conclude chiedendo in via principale che la richiesta della ricorrente venga dichiarata inaccoglibile, anche in considerazione del fatto che quest'ultima sarebbe legittimata ad agire nei confronti dell'autrice dell'illecito; in via subordinata, che si tenga conto delle somme già rimborsate alla cliente, ripartendo in ogni caso il danno fra le parti in proporzione alle rispettive responsabilità, ai sensi dell'art. 1227 c.c.

DIRITTO

La fattispecie in esame rientra nella tematica dell'uso non autorizzato di strumenti elettronici di pagamento e va dunque decisa sulla scorta delle disposizioni in materia, dettate dal d. lgs. 27 gennaio 2010, n.11, attuativo della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno europeo (c.d. "Direttiva PSD").
In via preliminare, va innanzitutto ricordato che le predette disposizioni disciplinano il rapporto tra i prestatori di servizi di pagamento e i propri clienti, prevedendo, con specifico riferimento alle operazioni di pagamento non autorizzate, che questi ultimi possano ottenere, al ricorrere delle condizioni che saranno appresso illustrate, il rimborso dei relativi importi. Va dunque disattesa l'eccezione di carenza di legittimazione passiva dell'intermediario, formulata in ragione dell'avvenuta individuazione dell'autore delle operazioni fraudolente (la domestica in servizio presso l'abitazione della ricorrente). Tale circostanza non vale infatti ad elidere il diritto della ricorrente ad agire nei confronti della banca prestatrice di servizi di pagamento, come quest'Arbitro, d'altro canto, ha già avuto occasione di affermare in analoghe circostanze (ABF Milano, dec. n. 969/2015).
Ciò premesso, va rammentato che, in punto di suddivisione delle responsabilità per operazioni di pagamento non autorizzate, il citato d.lgs. n. 11/2010 richiede che si valuti, da un lato, il comportamento del cliente rispetto agli obblighi di diligenza nella custodia dello strumento di pagamento e dei dispositivi ad esso collegati, dall'altro, la condotta dell'intermediario, tenuto ad adempiere al proprio mandato con la diligenza professionale e
qualificata dell'art. 1176, comma 2, c.c., attraverso la predisposizione di misure di sicurezza adeguate ai più evoluti standard tecnici. La legge mira, invero, sia a responsabilizzare l'utente di servizi di pagamento (inducendolo al rispetto di canoni comportamentali idonei ad impedire eventuali abusi ad opera di terzi), che ad obbligare gli intermediari ad adottare i sistemi di sicurezza più adeguati a prevenire possibili frodi.

Più in dettaglio, la normativa sopra citata disciplina, all'art. 12, la responsabilità del titolare dello strumento di pagamento per il caso di uso non autorizzato del medesimo, conseguente a smarrimento, sottrazione o indebito utilizzo (fattispecie all'interno delle quali è lecito ricomprendere, come correttamente osservato dalla ricorrente, anche l'ipotesi di mero utilizzo dei codici numerici e di altri dati identificativi della carta di pagamento, indipendentemente da una sua materiale apprensione ed utilizzazione presso un terminale fisico). Tale disposizione stabilisce, in particolare, che il titolare debba sopportare tutte le perdite derivanti da operazioni fraudolente poste in essere prima della comunicazione all'emittente dell'avvenuto furto o dell'uso non autorizzato, qualora abbia agito in modo fraudolento o non abbia adempiuto, con dolo o colpa grave, ad uno o più obblighi di cui all'articolo 7 (cioè, utilizzare lo strumento di pagamento in conformità alle disposizioni contrattuali che ne regolano l'emissione e l'uso; comunicare senza indugio al prestatore di servizi di pagamento, o al soggetto da questo indicato, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento; adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che consentono l'utilizzo dello strumento). Resta fermo, per altro verso, l'obbligo dell'intermediario di dimostrare la correttezza delle operazioni di pagamento sotto il profilo tecnico e contabile, il dolo o la colpa grave del cliente, nonché, in termini più generali, l'affidabilità del servizio erogato (gravando sul prestatore di servizi di pagamento, come sopra accennato, la responsabilità di eventuali falle nella sicurezza dei prodotti e degli strumenti forniti alla clientela).
Sulla scorta di tali principi va dunque decisa la controversia in esame, occorrendo stabilire se la ricorrente abbia violato, con grave ed inescusabile negligenza, gli obblighi di custodia dello strumento e di riservatezza dei dispositivi personalizzati (*password*) ad esso abbinati, o se, piuttosto, l'intermediario abbia contravvenuto all'obbligo di adeguare il servizio erogato agli standard di sicurezza più evoluti, secondo la tecnologia attualmente in uso.
L'indagine va condotta, peraltro, con riferimento all'unica operazione della quale non è stato offerto il rimborso alla ricorrente (ossia il pagamento *on line* di € 514,90 eseguito il 21/10/2016 alle ore 10:17), dovendosi considerare cessata la materia del contendere relativamente alle altre transazioni in contestazione (la resistente afferma infatti di avere eseguito, ed in altro caso offerto, il rimborso delle relative somme alla propria cliente, riconoscendo comunque il proprio debito).
Ora, con riferimento al comportamento della ricorrente, va osservato che dalla documentazione in atti emergono elementi sufficienti a far ritenere che quest'ultima non abbia osservato l'obbligo di conservare con cura il proprio strumento di pagamento e il codice personale (SecureCode MC) che ne consentiva l'uso su determinati siti, con ciò commettendo una grave ed inescusabile negligenza. È pacifico, invero, che tutte le operazioni contestate sono state poste in essere dalla collaboratrice domestica della ricorrente, che, frequentando liberamente l'abitazione della propria datrice di lavoro, avrebbe avuto tempo e modo di reperire la carta di credito di quest'ultima, di acquisirne i dati e di utilizzarli, nel corso di tre settimane circa, per effettuare ripetute transazioni *on line* (non necessitanti della disponibilità fisica della tessera, sempre rimasta, infatti, nella disponibilità della titolare). Quanto detto evidenzia una grave violazione degli obblighi di conservazione e di sicurezza dello strumento di pagamento gravanti sulla ricorrente, tenuta oggi a rispondere delle conseguenze dannose di comportamenti lesivi posti in essere da soggetti dalla stessa ammessi, evidentemente mal riponendo la propria fiducia, all'interno della sua personale sfera domestica (in questi termini, ABF Milano, dec. n. 6274/2015 e 969/2015). Tali conclusioni appaiono corroborate, peraltro, da quanto evidenziato nelle denunce presentate dalla stessa ricorrente, la quale afferma che all'interno della propria abitazione si erano verificati alcuni ammanchi di piccole somme; che la domestica, indebitata con terzi ed assillata dai creditori, avanzava insistenti richieste di denaro, lamentandosi altresì di non riuscire ad inviare soldi ai familiari nel

proprio paese d'origine; che la stessa era riuscita persino a scoprire la *password* di un dispositivo informatico della ricorrente; infine, che alcuni monili erano stati asportati da punti dell'abitazione noti solo alla padrona di casa: circostanze che, per un verso, avrebbero dovuto indurre la ricorrente ad una custodia particolarmente avveduta della carta e delle relative credenziali, confermando, per altro verso, che la collaboratrice domestica – la quale, come specificato nella denuncia, aveva le chiavi di casa e libero accesso a tutte le stanze, anche in assenza dei proprietari – era stata messa in condizione di poter frugare indisturbata in qualsiasi punto dell'appartamento. È più che plausibile, in conclusione, che la ricorrente abbia – sia pur involontariamente – consentito alla propria dipendente di reperire le proprie carte di pagamento, lasciate occasionalmente incustodite dentro casa, e di apprendere dati (estremi della carta, CVV e soprattutto *password*) che avrebbero dovuto restare rigorosamente riservati.
Non assume invece rilevanza, nella fattispecie, il ritardo (un mese circa) con il quale la ricorrente si è resa conto delle operazioni abusive poste in essere con la propria carta di credito e ne ha chiesto il blocco. L'obbligo di comunicare senza indugio all'emittente l'uso non autorizzato dello strumento di pagamento, invero, sorge non appena il titolare abbia avuto (o, si potrebbe sostenere, avrebbe dovuto avere) conoscenza del fatto (art. 7, par. 1, lett. *b)*). Sennonché, avendo la ricorrente mantenuto la disponibilità della propria carta, è difficile ipotizzare che la stessa, in mancanza di specifiche misure informative (come il servizio *sms alert*, su cui si veda appresso), potesse accorgersi sin da subito delle operazioni fraudolente e, segnatamente, riuscire a impedire il pagamento in contestazione.
Quanto invece alla condotta dell'intermediario, occorre innanzitutto rilevare che l'unica operazione ad oggi in contestazione sarebbe stata effettuata su un sito di "commercio elettronico sicuro", sul quale era necessario inserire, oltre ai dati indentificativi della carta (numero di serie, scadenza, nominativo del titolare, codice CVV2 stampato sul retro), il cd. SecureCode MC (come comprovato, nella specie, dalla cd. tracciatura dell'operazione, prodotta in atti). Tale circostanza giustificherebbe, dunque, il mancato rimborso della transazione abusiva, imputabile alla negligente custodia, da parte del titolare dello strumento, sia della carta che dei codici di sicurezza segreti ad essa abbinati.
È doveroso rilevare, tuttavia, che, secondo il consolidato orientamento di quest'Arbitro, la tecnologia "SecureCode" non è comunque ritenuta idonea a garantire un livello di sicurezza equiparabile a quello dei più evoluti presidi che è oggi possibile mettere a disposizione degli utilizzatori dei servizi di pagamento. Tale protocollo di sicurezza, invero, permette all'utente di associare alla propria carta una *password* personale e segreta (il SecureCode, appunto), richiesta per autenticare la transazione di pagamento ogni volta che si effettui un acquisto *on line* su un sito convenzionato. Non si tratta, tuttavia, di una *password* c.d. "dinamica", o di un sistema che genera *password* monouso di breve durata, in grado di elevare al massimo il livello di protezione dell'utente, bensì di una semplice *password* statica, come tale inidonea a limitare efficacemente i rischi di frode (tra le tante, v. ABF Milano, dec. n. 2771/16; ABF Napoli, dec. n. 174/16).
A ciò si aggiunga che, nel caso di specie, non risulta essere stato attivato neanche il servizio *sms alert*, presidio di sicurezza funzionale alla pronta rilevazione di operazioni non autorizzate, di uso ormai comune, che l'intermediario avrebbe quanto meno l'onere di proporre alla propria clientela, salvo espresso rifiuto da parte della stessa (ABF Roma, dec. n. 7714/16 e n. 2818/16). È infatti evidente che, se tale strumento fosse stato messo a disposizione della ricorrente, quest'ultima avrebbe potuto prevenire le transazioni abusive con carta di credito (quanto meno, quelle successive alla prima) attraverso una tempestiva comunicazione all'emittente, assumendosi, in caso contrario, la responsabilità della propria inerzia. La stessa ricorrente, d'altra parte, afferma di essersi insospettita proprio a seguito di un sms ricevuto dal proprio coniuge e di avere per tale motivo

effettuato i controlli dai quali erano emerse le operazioni di pagamento non autorizzate.
Ne discende, pertanto, che all'intermediario può essere rimproverata la violazione di quegli obblighi di diligenza professionale qualificata che gli impongono di predisporre i più adeguati ed evoluti sistemi di sicurezza in favore dei fruitori di servizi di pagamento dallo stesso offerti. Obblighi che appaiono conformi, del resto, anche al disposto dell'art. 8, lett. *a)* e *c)*, d. lgs. n. 11/2010, laddove si prevede, rispettivamente, che l'emittente lo strumento di pagamento debba assicurare che i dispositivi personalizzati che ne consentono l'utilizzo non siano accessibili a soggetti diversi da chi è legittimato ad usare lo strumento medesimo, e che siano sempre disponibili strumenti adeguati affinché l'utilizzatore del servizio di pagamento possa comunicare senza indugio all'intermediario il furto, lo smarrimento, l'appropriazione indebita o l'uso non autorizzato dello strumento di pagamento.
Alla luce di tali considerazioni, questo Collegio ritiene che la responsabilità dell'operazione di pagamento non autorizzata eseguita con la carta di credito della ricorrente possa essere
imputata ad entrambe le parti della presente controversia: se è vero, infatti, che le transazioni fraudolente in danno della ricorrente (compresa quella di € 514,90 tuttora in contestazione) non avrebbero avuto luogo, se la stessa avesse custodito con la dovuta attenzione i propri strumenti di pagamento (impedendo l'accesso ai relativi dati ad una persona di propria fiducia), è altrettanto vero che l'uso di un sistema di sicurezza maggiormente evoluto rispetto a quello utilizzato dall'intermediario (basato su una semplice *password* statica) e l'attivazione di ulteriori misure antifrode (come il sistema *sms alert*) avrebbero potuto con ogni probabilità scongiurare il compimento delle operazioni medesime (o, quanto meno, di quelle successive alla prima, tra le quali si colloca il pagamento *on line* in esame), nella specie agevolate, di contro, dalla scarsa efficacia dei presidi di sicurezza adottati dalla resistente.
Per tali ragioni, questo Collegio ritiene che, in applicazione della disciplina dettata dal citato d. lgs. n. 11/2010, nonché della regola generale di cui all'art. 1227 c.c. in materia di concorso colposo del creditore, le conseguenze dannose dell'operazione di pagamento non autorizzata eseguita con la carta di credito della ricorrente debbano essere equamente suddivise tra le parti, secondo le rispettive responsabilità. Il ricorso va dunque parzialmente accolto e l'intermediario dovrà corrispondere alla propria cliente l'importo di € 257,45, pari al 50% delle somme in contestazione.

P.Q.M.

Respinta ogni ulteriore istanza, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 257,45.