

Strumenti di pagamento – utilizzo fraudolento – responsabilità dell’intermediario – fattispecie (cod. civ., artt. 1710 e 1852; d.lgs. n. 11/2010, artt. 7, 8, 9 e 12)

La Banca risponde nei confronti del cliente dei danni causati dall'utilizzo fraudolento di uno strumento di pagamento quando non osserva i doveri di sicurezza e protezione del sistema imposti dal quadro normativo di riferimento. (MDC)

FATTO

La ricorrente lamenta che in data 6.7.2019, all'interno di un esercizio commerciale di vendita di calzature, alle ore 19.20 circa, le è stata sottratta da ignoti la borsa, che conteneva la carta prepagata a lei intestata. Gli ignoti malfattori sono poi riusciti ad effettuare, con la carta rubata, le seguenti operazioni: 1) alle ore 19:48, un prelievo ATM per € 250,00; 2) alle ore 19:50, altro prelievo ATM per € 350,00; 3) alle ore 20:13, un pagamento presso un'attività commerciale per € 300,00.

La ricorrente precisa che conservava "a memoria" il pin per l'utilizzo della carta, non lo custodiva unitamente alla carta, non lo ha fornito ad alcuno, né lo stesso era conosciuto da altri; aggiunge che non le è stato inviato alcun messaggio di alert, che avrebbe potuto evitare il compiersi delle operazioni fraudolente, consentendo di bloccare ancor più tempestivamente la carta.

Insoddisfatta dell'interlocuzione sviluppatasi con l'intermediario nella fase di reclamo, chiede pertanto le sia corrisposto dall'intermediario l'importo di € 900,00 corrispondente al valore delle tre operazioni di prelevamento.

Costitutosi, l'intermediario replica alle contestazioni avanzate in sede di ricorso osservando che: a) il primo prelievo di € 250,00 delle ore 19:48 è avvenuto con la digitazione immediatamente corretta del codice Pin, per cui i preposti sistemi informativi hanno riscontrato il tentativo di prelievo con il codice di risposta 000, e non con il diverso codice 117, generato automaticamente nel caso in cui venga rilevato un errore nella digitazione del codice; b) tutti i prelievi e pagamenti sono stati eseguiti con corretta e regolare lettura del microchip e non con banda magnetica; a tal proposito, la giurisprudenza dell'ABF ha più volte sostenuto che la tecnologia Emv, tramite cui è stata processata la carta intestata alla ricorrente, non permette di "leggere" il codice direttamente dalla carta se non tramite l'utilizzo di tecniche sofisticate, costose e connotate da tempi considerevolmente lunghi, circostanza di fatto incompatibile con la presente fattispecie in cui, al contrario, risulta sussistere sostanziale coincidenza temporale fra il momento del furto e quello del prelievo; nel reclamo presentato dalla parte ricorrente risultano, infatti, indicate le ore 19:20 come orario di consumazione del furto della borsa al cui interno era custodita la carta di pagamento oggetto della controversia.

L'intermediario richiama, a sostegno delle proprie deduzioni, la Circolare del 31 marzo 2015, Prot. n. 200413/AS, con la quale il Conciliatore Bancario Finanziario ha ufficialmente riferito gli esiti di un'indagine scientifica commissionata al Politecnico di Torino, nella quale veniva appurato che "data una carta Bancomat smarrita o rubata non è possibile con tempo e risorse limitate riuscire ad estrarre da essa il PIN contenuto nel chip. L'operazione è teoricamente possibile ma richiede un laboratorio sofisticato (chimico ed elettronico) e quindi ha un costo molto elevato ... e richiede comunque tempi molto lunghi (parecchie ore o giorni)"; richiama, inoltre, quanto stabilito dal Collegio di Coordinamento ABF nella Decisione 5304/2013, la cui fattispecie riguardava, in particolare, un caso di furto e prelievo a distanza di 12 minuti.

L'intermediario segnala infine di aver messo a disposizione dei propri clienti il servizio di sms Alert, che può essere attivato gratuitamente ed offre la possibilità di mantenere sotto controllo i movimenti relativi alla carta.

Chiede pertanto che il ricorso non sia accolto.

DIRITTO

La domanda della ricorrente è relativa all'accertamento del proprio diritto ad ottenere dall'intermediario emittente il rimborso di somme sottrattagli da ignoti mediante l'utilizzo fraudolento della carta di pagamento della quale era titolare, illecitamente sottrattagli mediante furto.

La materia, come noto, è regolata, oltre che dalle norme generali in tema di adempimento delle obbligazioni e sulla diligenza del mandatario (art. 1710 c.c.) e della banca nell'"esecuzione degli incarichi" (art. 1852 c.c.), dal d. lgs. n. 11/2010 il quale – al fine di favorire il corretto uso di strumenti di pagamenti diversi dal contante – impone una serie di obblighi tanto in capo all'utilizzatore, quanto in capo all'emittente.

In particolare, l'art. 7 impone che il primo utilizzi siffatti strumenti, conformemente alle prescrizioni contrattuali, in modo diligente, adottando misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo. Inoltre, l'art. 9 stabilisce l'obbligo da parte dell'utilizzatore avvedutosi di un'operazione fraudolenta di darne tempestivo avviso al prestatore dei servizi, mentre l'art. 12, comma 2, esonera da responsabilità, salvo il caso in cui abbia agito fraudolentemente, l'utilizzatore di uno strumento di pagamento, smarrito, sottratto o utilizzato indebitamente, nel caso in cui il prestatore di servizi di pagamento non abbia assicurato la piena fruibilità di strumenti atti consentire all'utilizzatore di comunicare senza indugio allo stesso prestatore l'utilizzo indebito dello strumento di pagamento.

Corrispondentemente, l'art. 8 impone a quest'ultimo di predisporre sistemi di sicurezza che non consentano l'accesso da parte di terzi ai dispositivi personali dell'utilizzatore e di impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta dal cliente ai sensi del citato art. 9.

L'evidente disparità di posizioni che le norme suddette comportano nei rapporti fra fornitore ed utente dei servizi di pagamento trova una giustificazione di natura sia sociale, sia commerciale, riconducibile al rischio, ossia all'idea secondo la quale è ragionevole far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose" che interessano una vasta platea di consumatori o di utenti, sull'impresa in quanto quest'ultima è in grado di distribuire su una moltitudine di utenti il rischio dell'impiego fraudolento di

carte di credito, di strumenti di pagamento, di conti correnti online, evitando che gravi direttamente ed esclusivamente sul singolo pagatore (sul punto v. ABF, Collegio di Coordinamento, nn. 6168/2013 e 3498/2012; recentemente, Collegio di Napoli, n. 1091/2018 e 10188/2018).

Peraltro, la concreta applicazione del principio non può prescindere da un'esatta delimitazione delle rispettive sfere di responsabilità del prestatore e dell'utilizzatore del servizio di pagamento.

Occorre, infatti, verificare, da una parte, se il fornitore abbia adottato tutti i migliori accorgimenti della tecnica per scongiurare tali impieghi fraudolenti, dall'altra, se l'eventuale negligenza del titolare dello strumento di pagamento sia tale da ricadere o meno nella nozione di colpa grave al cui ricorrere il summenzionato art. 12 d. lgs. n. 11/2010, esclude ogni responsabilità dell'intermediario.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede, come si è detto, una diversa distribuzione degli oneri probatori, in caso di furto o smarrimento degli strumenti di pagamento, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da dolo o colpa grave del cliente. Orbene, nel caso di specie dalla documentazione offerta in comunicazione dalle parti e, in particolare, dalla descrizione delle circostanze del furto e delle modalità di effettuazione delle tre operazioni abusive realizzate nell'arco di circa 25 minuti, prima del blocco della carta e della denuncia del fatto all'Autorità di P.S. e, soprattutto, dalla mancata attivazione del servizio di sms alert, emerge che l'intermediario non abbia dimostrato di aver puntualmente assolto ai suoi doveri di sicurezza e protezione del sistema posti dalla richiamata normativa.

Giova al riguardo richiamare quanto stabilito dal Collegio di Coordinamento nella decisione n. 24366/2019 secondo cui "l'attivazione del servizio di "sms-alert" costituisce un onere gravante direttamente sull'intermediario, a prescindere dal fatto che il cliente ne abbia o meno richiesto l'attivazione".

In questa prospettiva, che il Collegio condivide, "la mancata attivazione del servizio di "sms-alert" costituisce (...) una carenza organizzativa imputabile all'intermediario (..) il quale, data la natura di misura di sicurezza del sistema di sms alert, non dovrebbe limitarsi a proporlo al cliente ma dovrebbe adottarlo in modo generalizzato", come invece accaduto nel caso qui in esame.

In considerazione di quanto precede, considerato che l'attivazione del servizio non avrebbe potuto comunque impedire la prima delle tre operazioni abusive (dell'importo di € 250,00), il Collegio reputa il ricorso meritevole di parziale accoglimento

P.Q.M.

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo di € 650,00 (....omissis...).