

IL COLLEGIO DI COORDINAMENTO

composto dai Signori:

Dott. Giuseppe Marziale Presidente del Collegio ABF di Roma	Presidente
Prof. Avv. Antonio Gambaro Presidente del Collegio ABF di Milano	Membro effettivo
Prof. Avv. Enrico Quadri Presidente del Collegio ABF di Napoli	Membro effettivo
Prof.ssa Lucia Picardi Componente del Collegio ABF di Napoli designato dal Conciliatore Bancario Finanziario (per le controversie in cui sia parte un cliente consumatore)	Membro supplente [Relatore]
Avv. Pierfrancesco Bartolomucci Componente del Collegio ABF di Napoli designato dal CNCU	Membro effettivo

nella seduta del 18/12/2013, dopo aver esaminato

- il ricorso e la documentazione allegata;
- le controdeduzioni dell'intermediario e la relativa documentazione;
- la relazione istruttoria della Segreteria tecnica,

FATTO

Con atto datato 28 dicembre 2012 ed identificato con n. prot. 1103066/12, il ricorrente si rivolgeva all'Arbitro Bancario Finanziario deducendo di essere titolare di una carta di debito rilasciata dall'intermediario resistente e rimasta sempre "*depositata nel comodino della camera da letto, unitamente al codice PIN*" senza essere stata mai utilizzata. In data 30 luglio 2012, all'arrivo dell'estratto conto del mese di giugno, il ricorrente medesimo si era avveduto, però, di 12 prelievi presso due ATM (a Flero e a Brescia). Il giorno successivo, prima di sporgere denuncia, egli si era recato presso l'ufficio dell'intermediario ed aveva constatato ulteriori 8 prelievi fraudolenti, compiuti nel mese di luglio.

Il ricorrente presumeva, pertanto, la clonazione dello strumento di pagamento. Nel ricorso dichiarava di essere ipovedente e di aver custodito “*con la massima cura*” il codice PIN, sicché nessuna persona “*di casa*” aveva potuto accedere a tali dati; rilevava, infine, che i prelievi erano stati spesso effettuati in successioni di un minuto.

Replicava l'intermediario che la carta di debito, per la quale l'interessato asseriva la clonazione, era una carta di pagamento “*dotata di microchip di ultima generazione*”. Tale carta era stata consegnata al cliente il 21.05.2012 in sostituzione di una precedente carta, bloccata dal titolare presso la Centrale d'allarme. In passato il ricorrente si era lamentato più volte di fenomeni analoghi, tanto da aver bloccato nel 2012 due carte di pagamento (il 19.03.2012 e il 03.05.2012). Sottolineava come non risultassero per la carta oggetto di contestazione evidenze informatiche e contabili riconducibili a fattispecie note di clonazione carta, né altri elementi d'irregolarità delle operazioni, sia formali che sostanziali. Le operazioni erano state compiute osservando correttamente le procedure di sicurezza anticlonazione (codici random sequenzialmente registrati sulla carta ad ogni operazione; saldi storici dei prelievi presso ATM): ciò dimostrerebbe l'uso del dispositivo originale. Le operazioni contestate erano state disposte in un lasso temporale molto lungo, in orari di ordinaria operatività e nelle vicinanze della residenza del titolare della carta. Indizi tutti, che lascerebbero ricavare una grave negligenza nella custodia della carta. Il ricorrente chiedeva il rimborso di quanto sottrattogli a seguito dell'uso fraudolento della propria carta di debito: € 5.250,00, mentre l'intermediario insisteva per il rigetto del ricorso.

La controversia veniva presa in esame dal Collegio di Milano nella seduta del 5.9.2013, nella composizione prescritta per la trattazione dei ricorsi promossi dai consumatori. In quell'occasione il Collegio, rilevata la presenza di orientamenti contrastanti nelle decisioni dell'ABF, rimetteva il ricorso all'esame del Collegio di coordinamento al fine di chiarire, in particolare, se la disciplina dettata dal d. lgs. n. 11/2010, emanato in attuazione della direttiva 2007/64/CE, trovi applicazione non solo nei casi (testualmente previsti) di furto, smarrimento o utilizzo non autorizzato di una carta di pagamento, ma anche nel caso della clonazione ad opera di terzi malfattori, con conseguente onere del fornitore di servizi di pagamento di fornire la prova della colpa grave dell'utilizzatore.

DIRITTO

Il ricorrente è titolare di una carta di debito emessa dalla convenuta e collegata al proprio conto corrente. Tale carta è dotata di microchip e funziona tramite digitazione di un

PIN segreto, che viene attribuito in via esclusiva al possessore dello strumento Al caso di specie va applicabilità la disciplina del d. lgs dal momento che i fatti da cui è scaturita la presente controversia si sono svolti successivamente al 1° marzo 2010, data di entrata in vigore del sopra menzionato decreto legislativo.

Così individuato il quadro normativo di riferimento, occorre chiarire quale sia l'ambito di responsabilità del prestatore di servizi di pagamento a fronte del disconoscimento da parte dell'utilizzatore dei servizi medesimi di un'operazione di pagamento già eseguita o della contestazione circa la corretta esecuzione della stessa. Come è già stato chiarito dal Collegio di coordinamento (cfr. la decisione n. 3498/2012), la normativa testé richiamata istituisce un regime di speciale protezione e di altrettanto speciale *favor probatorio* a beneficio degli utilizzatori, che si ricava dalle seguenti proposizioni precettive (art. 10 d. lgs. n. 11/2010): a) in caso di disconoscimento di un'operazione di pagamento, è onere del prestatore dei servizi di pagamento provare che essa è stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non si deve a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema; b) l'apparentemente corretta autenticazione non è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la disconosca; c) la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi che l'art. 7 del decreto pone a suo carico e che si limitano all'utilizzazione dello strumento di pagamento in conformità alle condizioni contenute nell'accordo quadro che regola il servizio e alla tempestiva denuncia di furto, smarrimento, distruzione o altro uso non autorizzato dello strumento. Laddove una simile responsabilità non possa affermarsi, l'utilizzatore non sopporterà le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento, se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 150 euro (art. 12, commi 1 e 3, d. lgs. n. 11/2010).

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 "social-commerciale" riconducibile – come è stato affermato da questo Collegio di coordinamento (cfr. decisione n. 3498/2012), sulla scorta di una pronuncia del Collegio di Roma (decisione n. 1111/2010) – al rischio d'impresa, 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 tale moltitudine il rischio dell'impiego

fraudolento di carte di credito o di strumenti di pagamento, evitando che gravino direttamente ed esclusivamente sul singolo pagatore.

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 – di là dall'ipotesi in cui la condotta del cliente sia connotata dal dolo, sì da escludere l'operatività di qualsivoglia presidio – 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 esclude ogni responsabilità dell'intermediario.

A questo proposito, il Collegio di Milano ha in numerose occasioni ritenuto dirimente il riscontro fornito dall'intermediario che la carta di pagamento utilizzata per prelievi di contante fosse dotata di *microchip* di ultima generazione; elemento, questo, che rende “tecnicamente e statisticamente remota e trascurabile la possibilità di una clonazione”, la cui prova – in base a quanto statuito dall'art. 2697 c.c. – deve essere fornita dal ricorrente (Collegio ABF di Milano, decisioni n. 561/2013; n. 2571/2012). Tale posizione è condivisa dal Collegio di Napoli, ad avviso del quale la circostanza che le operazioni contestate siano avvenute mediante l'utilizzo esclusivo della tecnologia a microcircuito di cui la carta è dotata esclude in radice (almeno allo stato attuale delle conoscenze in materia) la possibilità della clonazione dello strumento di pagamento utilizzato, salvo che il ricorrente fornisca, sia pure in via presuntiva, elementi atti a corroborare il fatto dedotto (Collegio ABF di Napoli, decisioni n. 1802/2013, n. 275772012).

Diversamente orientato è, invece, il Collegio di Roma, che tende a respingere l'assunto secondo il quale la clonazione è fatto la cui dimostrazione incomberebbe in linea di principio al cliente e sostiene invece che, essendovi alla base del rilascio di carte di pagamento con addebito in conto corrente un rapporto contrattuale fra l'intermediario ed il cliente, ove questi si dolga nei confronti del primo dell'inadempimento degli obblighi di custodia e salvaguardia del denaro del cliente stesso, è l'intermediario – in base ai principi scolpiti nell'art. 1218 c.c. – a dover provare di aver adempiuto a siffatti obblighi con la diligenza professionale qualificata, identificata dalla ormai costante giurisprudenza come “diligenza del buono ed accorto banchiere”. Poste tali premesse, il citato Collegio considera detto onere non assolto dall'intermediario qualora quest'ultimo si limiti ad escludere la clonabilità delle carte che utilizzano il sistema a *microchip* e a presumere la negligente custodia, da parte del cliente, della carta e dei relativi codici dispositivi (Collegio

ABF di Roma, decisione n. 960/2012). Lungo l'indicata linea argomentativa, il Collegio assume, altresì, che l'intermediario debba farsi carico di accertare, attraverso l'identificazione dei codici randomici delle operazioni compiute con la carta di cui si ipotizza la clonazione, se detti codici attestino la continuità e la consequenzialità fra le operazioni poste in essere con la digitazione del medesimo PIN, continuità tale da poter escludere con sufficiente certezza che esse siano state poste in essere con due supporti materiali diversi, ossia con due diverse carte, quella originale ed il suo clone (cfr. Collegio ABF di Roma, decisione n. 260/2011). Ne discende che laddove l'intermediario si limiti ad escludere l'ipotesi della clonazione della carta, ventilata invece dal cliente, senza fornire alcuna evidenza probatoria in tal senso, quest'ultimo potrà sopportare la perdita derivante dall'indebito utilizzo dello strumento di pagamento solo entro il limite di cui all'art. 12, comma 3, d.lgs. 11/2010 (cfr. Collegio ABF di Roma, decisione n. 292/2013). Tale soluzione presuppone un indirizzo interpretativo favorevole ad applicare la norma appena citata, oltre ai casi testualmente previsti di furto, smarrimento o utilizzo non autorizzato di una carta di pagamento, anche nell'ipotesi di clonazione della medesima ad opera di terzi malfattori (Collegio ABF di Roma, decisione n. 3573/2012).

Va tuttavia aggiunto che il regime ordinario di responsabilità limitata dell'utente dei servizi di pagamento incontra talune eccezioni indicate nel successivo quarto comma dello stesso art. 12 e consistenti nell'aver agito in modo fraudolento o nel non aver adempiuto ad "uno o più obblighi di cui all'art. 7" con dolo o colpa grave. Non si può negare che rispetto al dolo e alla frode, la fattispecie della colpa grave è più difficilmente definibile. Non può essere revocato in dubbio che la presenza di un comportamento gravemente colpevole dell'utente deve essere provata dal fornitore del servizio, il quale sarà tenuto ad allegare indizi precisi e concordanti che supportino tale qualificazione, mentre il mero fatto che sia stato utilizzato il dispositivo di sicurezza dell'utente non può configurare una grave negligenza, come è chiarito dall'art. 10, comma 2. Pur nella consapevolezza che un'interpretazione eccessivamente ampia delle fattispecie sussumibili entro la sfera della colpa grave potrebbe ridimensionare la portata del regime di responsabilità "*consumer friendly*" di cui la disciplina in esame è espressione, i tre Collegi ABF ammettono la possibilità di accertare la grave negligenza in via presuntiva, escludendo conseguentemente l'ipotesi di una clonazione sul presupposto che ricorrano elementi gravi, precisi e concordanti ex art. 2729 .c. c.

Alla luce di tali considerazioni, si può fondatamente argomentare la sussistenza di un comportamento negligente destinato ad assumere un rilievo assorbente e determinante



nella concreta concatenazione degli eventi, ogniqualvolta l'utente abbia ommesso di custodire il codice PIN separatamente dalla carta, in violazione dei patti, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso. Tale circostanza, nel caso di specie, è pacificamente ammessa dal ricorrente, il quale ha dichiarato di aver sempre custodito la carta di pagamento "nel comodino della camera da letto unitamente al codice PIN senza mai utilizzarla", presumendo, quindi, che la stessa sia stata illecitamente clonata da terzi. Dinanzi ad un così palese inadempimento degli obblighi di custodia e segretezza dei codici dispositivi posti a suo carico, il ricorrente non potrà non incorrere in una responsabilità illimitata, sicché le perdite subite nella propria sfera patrimoniale non possono ricevere alcun ristoro da parte dell'intermediario.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
GIUSEPPE MARZIALE