COLLEGIO DI BOLOGNA- DECISIONE n. 6987/2017 – PRES. MARINARI – REL. MARINARO

Servizi di pagamento – home banking- operazione non autorizzata – phishing – contestazione - sistemi di sicurezza – assenza di prova – accoglimento (d.Lgs. 11/2010, artt. 5, 7, 10 e 12)

FATTO

Il ricorrente espone di essere titolare di una carta di credito rilasciata dalll'intermediario resistente. In data 10/05/2016 riceveva, all'indirizzo di posta elettronica fornito all'intermediario resistente al momento della registrazione, una e-mail contenente un avviso di "tentata intrusione" sulla predetta carta.

In considerazione del ben noto fenomeno del phishing, ed essendo, inoltre, dipendente della Polizia di Stato e, dunque, particolarmente avvezzo a trattare (e conoscere) i vari fenomeni di truffa online in ragione della propria esperienza lavorativa, ben si guardava dal rispondere a tale email.

Provvedeva, pertanto, a contattare l'ufficio clienti dell'intermediario resistente e, sotto la guida dell'operatore di turno, modificava la propria password 3D Secure tramite il sito ufficiale dell'intermediario resistente. L'intermediario resistente confermava l'avvenuta modifica della predetta password con e-mail del 10/05/2016.

Successivamente, in data 13/05/2016, accedeva casualmente alla propria home banking, per verificare, come è solito fare, l'estratto conto relativo alla carta, e notava una transazione, dal medesimo non autorizzata, dell'importo di € 1.012,95, a favore del sito di una nota marca di abbigliamento.

Il medesimo giorno (13/05/2016), non appena appreso dell'illecita sottrazione, sporgeva denuncia - querela per l'accaduto ed effettuava il blocco della suddetta carta; inoltre, il 16.5.2016 provvedeva a presentare reclamo all'intermediario resistente, dapprima, oralmente, (contattando telefonicamente l'ufficio clienti dell'intermediario) e, successivamente, dietro richiesta di quest'ultimo, formalizzando il reclamo per iscritto, utilizzando un apposito modulo mandatogli, a tale scopo, dall'intermediario al proprio indirizzo email.

Qualche tempo dopo, si accorgeva che sul frontespizio della nota di risposta alla contestazione, inviatagli dall'intermediario all'indirizzo email corretto, era indicato un diverso indirizzo email, a lui non riferibile; pertanto, con comunicazione del 17/06/2016, ad integrazione del reclamo, contestava la circostanza all'intermediario disconoscendo l'indirizzo come a se riconducibile.

Con email del 24/06/2016, l'intermediario, tuttavia, respingeva il reclamo addebitando l'operazione disconosciuta all'incauta custodia da parte del ricorrente sia della carta che delle relative credenziali, avendo il ricorrente risposto ad una e-mail di phishing.

"A seguito di tali infondate ed apodittiche conclusioni", il ricorrente replicava a mezzo difensore tecnico ribadendo la propria estraneità ai fatti; il ricorrente ritiene che la vicenda in questione vada ricondotta ad una truffa a mezzo internet ove un ignoto truffatore, utilizzando una email a lui non riferibile, è riuscito a modificare i codici d'accesso alla sua home banking, sottraendogli, in tal modo, l'importo di € 1.012,95.

Il ricorrente afferma, infatti, che non gli sia imputabile alcun comportamento negligente e/o colposo nella custodia della carta né delle credenziali avendo custodito la carta di credito con la massima diligenza e avendo adottato tutte le cautele idonee e necessarie ad evitare che estranei entrassero in possesso del numero identificativo e dei codici personalizzati che consentono l'utilizzo della carta.

Al riguardo, rileva che il fatto che la transazione sia stata operata tramite la corretta

digitazione dei dati della carta e della password 3D Secure, non esclude, la possibilità di un utilizzo fraudolento dello strumento di pagamento da parte di terzi. Né la circostanza di aver aderito al servizio “Verified by Visa” può considerarsi elemento idoneo a comprovare il dolo o la colpa grave del cliente nella custodia delle credenziali come anche rilevato dai Collegi ABF, che hanno affermato che il sistema 3D Secure “presenta indubbiamente elementi di sicurezza in quanto richiede una password, ma non è considerato un sistema a tal punto sicuro da escludere la possibilità di un’intrusione da parte di terzi.”
L’intermediario resiste al ricorso e rileva:
• quanto alla email ricevuta dal ricorrente in data 10/05/2016, si è trattato evidentemente, di una email di phishing;
• riguardo a quanto accaduto in seguito alla ricezione della predetta email, il ricorrente ha fornito versioni contrastanti: nella denuncia presentata all’Autorità giudiziaria ha affermato che a seguito della ricezione di tale email, contattava il sito web dell’intermediario (… in cui vi erano dei passaggi per aggiornare la carta e che fosse sicuro dell’autenticità e dell’attendibilità di tale sito), nel ricorso, ha affermato di non aver risposto alla predetta email e di aver chiamato, invece, il servizio clienti dell’intermediario;
• tale contatto ha avuto ad oggetto esclusivamente il reset della password di accesso al portale titolari;
• inoltre, in data 11/05/2016 è stato variato il numero di cellulare dove ricevere il codice OTP, necessario per perfezionare le operazioni di acquisto on line mediante l’area riservata del portale titolari;
• pertanto, qualcuno, che si era evidentemente già impossessato delle credenziali per accedere all’area riservata del portale titolari (molto probabilmente chi ha spedito l’email di phishing), si è collegato al sito web dell’intermediario e ha modificato l’utenza del ricorrente inserendo le informazioni necessarie per poter compiere la frode ed in particolare, il numero di cellulare ove ricevere il codice OTP necessario a perfezionare l’operazione on line.
L’intermediario riferisce inoltre:
• di aver messo a disposizione dei propri clienti tutti gli strumenti possibili per rendere sicure le operazioni di pagamento, sia on line che nel mondo fisico;
• in particolare, con riguardo al caso di specie, la transazione disconosciuta dal ricorrente è una transazione on line, che si è conclusa secondo le regole del 3D Secure, protocollo di sicurezza voluto dai circuiti internazionali per dare maggiore tutela ai clienti che utilizzano la carta di credito per acquisti in internet.
Nello specifico, il suddetto protocollo prevede che:
- al momento dell’acquisto vengono inseriti i dati della carta di credito e del cliente;
- alla conferma dell’acquisto il cliente riceve, via SMS sul cellulare registrato presso il portale titolari, un OTP (one time password) sotto forma di codice numerico;
- questo codice deve essere inserito nell’apposito spazio riservato e, una volta data la conferma, se il codice è corretto, il sistema convalida;
• il sistema di monitoraggio delle transazioni, attivo 24 h, non ha rivelato alcuna anomalia, in quanto tutti i passaggi si sono svolti in piena conformità.

DIRITTO

1. - La controversia origina dalla richiesta di ripetizione di somme sottratte mediante l’utilizzo fraudolento della carta di credito della parte ricorrente.
Il ricorrente in particolare disconosce un’operazione di pagamento dell’importo di € 1.012,95 effettuata in data 13/05/2016 mediante la sua carta di credito, sul sito web di una nota marca di abbigliamento.
Nella denuncia sporta per l’accaduto il ricorrente ha dichiarato di essersi accorto della suddetta transazione intorno alle ore 12.00 del 13/05/2106 e di avere provveduto a

bloccare la carta , ricevendo, a tal fine, un codice di blocco.
Il ricorrente sostiene che un ignoto truffatore, utilizzando una email a lui non riferibile sia riuscito a modificare i codici d'accesso alla sua home banking, sottraendogli, in tal modo, l'importo di € 1.012,95. A sostegno di ciò, produce il modulo di reclamo inviatogli dall'intermediario recante il suddetto indirizzo email.
L'intermediario ha prodotto il log dell'operazione contestata da cui emerge che è stata effettuata il 13/05/2016 alle ore 11.44.08.
L'intermediario si difende sostenendo che il ricorrente ha risposto, molto probabilmente, ad una email di phishing e fa presente, inoltre, che l'operazione disconosciuta è stata eseguita secondo le regole del 3D Secure, protocollo di sicurezza voluto dai circuiti internazionali.
L'intermediario afferma, in particolare, che la transazione disconosciuta dal ricorrente si è correttamente conclusa mediante l'inserimento nel sistema di un codice OTP, inviato al numero di telefono cellulare associato alla carta e che tale numero era stato modificato.
Dalla documentazione prodotta dall'intermediario resistente emerge, invero, che tra il 10/05/2016 e il 13/05/2016 l'utenza telefonica abbinata alla carta è stata cambiata più volte: il 10/05/2016 alle ore 11.33, mediante contact center; il 11/05/2016 alle ore 17.19, mediante il portale titolari; il 13/05/2016 alle ore 11.30, mediante il portale titolari; il 13/05/2016 alle ore 11.46, mediante il portale titolari.
Precisamente, tra il 10/05/2016 e il 13/05/2016 l'utenza telefonica associata alla predetta carta è stata cambiata per 4 volte, venendo indicati 4 numeri di telefono diversi e non risulta che tale la circostanza sia stata oggetto di valutazione da parte dell'intermediario ai fini di un possibile rischio di frode.
2. - Il Collegio, nella riunione del 28.3.2017, rilevato, sulla base della documentazione prodotta dall'intermediario, che tra il 10.5.2016 e il 13.5.2016 l'utenza telefonica associata alla predetta carta era stata cambiata per 4 volte, venendo indicati 4 numeri di telefono diversi, sospendeva il procedimento rivolgendo una richiesta di integrazione documentale all'intermediario e più precisamente:
«Il Collegio, ritenuta la necessità di una integrazione istruttoria ai fini della decisione del ricorso, richiede all'intermediario di chiarire e di documentare nel termine di quindici giorni dalla ricezione della presente comunicazione quale fosse all'epoca dei fatti la procedura seguita nei casi di modifica del numero di cellulare per la ricezione del codice OTP e dell'indirizzo mail indicati dal cliente nell'area riservata del portale, precisando le modalità di comunicazione al cliente della modifica di tali dati».
2.1. - L'intermediario, in data 14.4.2017, ha fornito risposta alla richiesta senza produrre alcuna ulteriore documentazione (tantomeno la copia del contratto con le condizioni concordate di utilizzo del servizio).
Nella nota di risposta si legge che all'epoca dei fatti (maggio 2016) «la variazione del numero di cellulare se fatto dal Servizio Clienti non generava, come invece accade oggi, un SMS di avviso inviato al precedente numero di cellulare, in quanto la modifica era subordinata ad una minuzionosa identificazione di chi faceva la richiesta. Nel caso di variazione da Portale Titolari, veniva invece inviato al Cliente un SMS di avviso sul vecchio numero. Evidenziamo comunque che la modificazione poteva – e tuttora può – essere fatta solo accedendo all'area profilata del portale riservato ai titolari grazie alle chiavi di sicurezza che dovrebbero essere custodite con cura e note solo al cliente e, quindi, in grado di garantire che ad operare il cambio di numero di cellulare sia il legittimo titolare della carta di credito»
Si aggiunge in detta nota che in relazione alla modifica dell'indirizzo di posta elettronica «tale attività non prevedeva, né prevede tuttora, l'invio di alcuna informativa e ciò perché questa operazione può essere portata a termine dal cliente medesimo accedendo con le proprie chiavi di sicurezza, oppure facendo richiesta al nostro Servizio Clienti che, previa

accurata identificazione attraverso la raccolta di diversi dati e codici in possesso del cliente, evade la richiesta».
2.2. – Rileva il Collegio in via preliminare che l'esito fornito dall'intermediario appare generico e per ciò stesso insufficiente. Nessuna documentazione contrattuale è stata prodotta circa i sistemi di protezione, di accesso e di autenticazione al "portale titolari" che consentono di modificare dati (in particolare il numero di cellulare) che a loro volta consentono poi di carpire il c.d. O.T.S. (codice inviato via sms).
Peraltro, l'intermediario sostiene senza documentarlo che, in caso di variazione dal "Portale Titolari" del numero di cellulare abbinato alla carta, sarebbe stato inviato un SMS di avviso al vecchio numero di telefono. Non vi è né documentazione contrattuale sul punto né la prova dell'invio e della corretta consegna del messaggio relativo alle modifiche effettuate. Resta fermo che si tratta di mere notifiche di avvenuta modifica, non essendo previsti sistemi di autorizzazione mediante l'utilizzo di diversi canali di comunicazione utili a meglio proteggere il cliente da una tipologia di truffe divenute rapidamente sempre più frequenti in quanto sfruttano un evidente vulnus del sistema di accesso medianti chiavi statiche al "portale titolari".
3. - La disciplina di riferimento per la soluzione del caso sottoposto all'esame di questo Collegio è contenuta nel D.lgs. 11/2010 ed in particolare negli artt. 5, 7, 10 e 12.
In base all'art. 5, co. 1 e 2, D.lgs. 11/2010 «Il consenso del pagatore è un elemento necessario per la corretta esecuzione di un'operazione di pagamento. In assenza del consenso, un'operazione di pagamento non può considerarsi autorizzata» ed «Il consenso ad eseguire un'operazione di pagamento o una serie di operazioni di pagamento è prestato nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento».
Ai sensi dell'art. 7, comma 1, lett. a) e b), D.lgs. 11/2010 (che individua gli obblighi a carico dell'utilizzatore dei servizi di pagamento in relazione agli strumenti di pagamento), «L'utilizzatore abilitato all'utilizzo di uno strumento di pagamento ha l'obbligo di: a) utilizzare lo strumento di pagamento in conformità con i termini, esplicitati nel contratto quadro, che ne regolano l'emissione e l'uso; b) comunicare senza indugio, secondo le modalità previste nel contratto quadro, 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 non appena ne viene a conoscenza».
L'art. 10 D.lgs. 11/2010 codifica poi l'inversione dell'onere della prova: «1. 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. - 2. 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».
Infine, secondo quanto statuito dall'art. 11, co. 1, D.lgs. 11/2010 (e fatto salvo l'art. 9), «nel caso in cui un'operazione di pagamento non sia stata autorizzata, il prestatore di servizi di pagamento rimborsa immediatamente al pagatore l'importo dell'operazione medesima».
4. - Nel caso di specie appare evidente che l'intermediario pur avendo esibito il "log" dell'operazione non ha fornito prova che il ricorrente abbia effettivamente autorizzato l'operazione in contestazione.

Mediante il c.d. "log" l'intermediario ha provato l'utilizzo di uno strumento di pagamento

registrato, ma la sola produzione del medesimo “log” non è sufficiente a consentire di ritenere «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».
Ed infatti, si rileva dall’istruttoria come la parte ricorrente abbia provveduto a richiedere il blocco della carta di credito con immediatezza e che poi abbia presentato denuncia dell’accaduto. Né vi sono ulteriori elementi che possano far ritenere che ragionevolmente il cliente sia venuto meno agli obbligi di custodia della carta di credito e delle credenziali di accesso al “portare titolari”.
Né appare possibile desumere dalla descrizione dei fatti del ricorrente versioni difformi tali far emergere contraddizioni ricostruttive utili ad un convincimento necessario a ritenere sussistente la colpa grave a carico dello stesso. Infatti, la versione resa in sede di denuncia è molto più breve (come sempre accade data la modalità di acquisizione di tali dichiarazioni e delle finalità che ad essa conseguono) e consente di rilevare come il cliente abbia “contattato il sito web” dell’intermediario (precisando di essere sicuro che lo stesso fosse quello “attendibile”). Nel ricorso invece fornisce una più ampia e dettagliata ricostruzione allo scopo di fornire ulteriori elementi di comprensione della vicenda, ma senza sostanzialmente contraddirsi in quanto precisa di essersi anche rivolto telefonicamente all’assistenza clienti (il contatto telefonico è circostanza confermata dall’intermediario) tramite il numero verde «reperito sul sito ufficiale …» e guidato poi dall’operatore di turno avrebbe modificato la password 3D secure (il reset della pasword nel giorno indicato dal ricorrente è confermato dall’intermediario).
5 - L’intermediario resistente precisa che l’operazione contestata è stata disposta su un sito internet il cui esercente è stato censito come “sicuro” e certificato ad effettuare solo operazioni che necessitano dell’autenticazione del partecipante. In particolare, l’operazione disconosciuta sarebbe stata disposta attraverso il sistema 3D-Secure (verified by Visa), che inibisce l’utilizzo della carta di credito in assenza di autorizzazione del titolare, prevedendo il sistema in questione l’inserimento del codice titolare, del codice riportato sul retro della tessera e del codice OTS.
La transazione, inoltre, sarebbe avvenuta su un sito internet qualificato da appositi protocolli di sicurezza previsti da circuiti internazionali, che permettono l’esecuzione di transazioni mediante l’utilizzo di credenziali note unicamente al titolare della carta.
I Collegi ABF hanno avuto modo di affrontare analoghe controversie rilevando come anche con l’adesione al servizio “Verified by Visa” non possa considerarsi fornita ipso facto prova certa dell’elemento del dolo o colpa grave del ricorrente, la cui presenza soltanto potrebbe integrare la sua responsabilità per l’accaduto. Non è invero escluso che una intrusione illecita nel sistema sia comunque potuta avvenire (ABF Coll. Roma, dec. n. 1904/2014; dec. n. 562/2015).
6. – Invero, un sistema multifattore con chiave dinamica al portale ed un sistema di autorizzazione protetto di modifica dei dati che concorrono all’attività dispositiva della carta di credito avrebbero concorso sicuramente ad apprestare una più elevata protezione al titolare della carta utile a prevenire simili tipologia di frodi. Come anche il monitoraggio costante non soltanto delle operazioni dispositive, ma degli accessi al portale titolari avrebbe consentito di rilevare questi rischi di frode (si pensi, ad es., al cambio rapido e ripetuto del numero di cellulare, ma anche dell’indirizzo di posta elettronica, quali evidenti elementi sintomatici di un rischio di frode che possono condurre ad un blocco cautelativo ex art. 6, comma 2, lett. b, D.lgs 11/2010).
L’evoluzione costante dei metodi utilizzati per carpire le credenziali informatiche nell’utilizzo delle carte di pagamento (che sfruttano i punti deboli sei sistemi di protezione, come nel caso di specie, dell’accesso al “portale titolari” per la modifica del numero di cellulare ove ricevere la chiave dispositiva OTS azzerandone l’efficacia di strumento di

sicurezza), impone una costante attenzione, una puntale analisi ed una incessante evoluzione dei connessi sistemi di protezione del cliente. Qualora i clienti nell'utilizzo di questi sistemi dovessero ritenersi non sufficientemente protetto, inizierebbero a limitarne sino a dismetterne totalmente il loro utilizzo con buona pace della diversa esigenza di rafforzare e diffondere gli strumenti elettronici di pagamento.
Di qui la scelta legislativa dell'inversione dell'onere della prova e del rigore imposto nella valutazione della colpa grave a carico dell'utilizzatore (cfr. Coll. Coord., dec. n. 3498/2012, sulla scorta della decisione del Coll. Roma, dec. n. 1111/2010 e poi Coll. Coord., dec. n. 991/2014) allocando quindi sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento (Coll. Coord., dec. n. 3947/2014).
7. – Pertanto, nella fattispecie in esame, dai fatti rappresentati in narrativa e dalle evidenze disponibili acquisite nel contraddittorio tra le parti, emerge che il ricorrente non ha autorizzato l'operazione contestata e che probabilmente è stato vittima di una macchinazione fraudolenta da parte di terzi malfattori, avente una modalità particolarmente sudbdola ed invasiva. Se ciò è accaduto, è stata la conseguenza di un sistema di protezione scarsamente sicuro apprestato dall'intermediario il quale seppur ha previsto un meccanismo di autenticazione dell'operazione multifattore con chiave dinamica (c.d. 3D Secure con OTS), non ha adegutamente protetto l'accesso al "portale titolari" dotato di un sistema ad unico fattore con chiave statica e che consente la modifica di dati da utilizzare per effettuare operazioni (azzerando di fatto la protezione della chiave dinamica mediante OTP da utilizzare per la fase dispositiva). Per cui, anche a voler ammettere che possa ravvisarsi nel comportamento del ricorrente una colpa, quest'ultima non è pertanto suscettibile di essere qualificata come "grave".
Secondo l'insegnamento della Suprema Corte, la colpa grave è costituita infatti da una «*straordinaria e inescusabile*» imprudenza, negligenza o imperizia, la quale presuppone che sia stata violata non solo la diligenza ordinaria del buon padre di famiglia di cui all'art. 1176, comma 1, c.c., ma anche «*quel grado minimo ed elementare di diligenza generalmente osservato da tutti*» (Cass., 3 maggio 2011, n.913; Cass., 19 novembre 2001, n.14456).
In difetto di tale prova questo Collegio considera pertanto l'operazione di pagamento di cui si discute come non autorizzata dal ricorrente e, pertanto, a lui non opponibile, con conseguente sussistenza di un dovere di integrale rimborso in capo all'intermediario ai sensi e nelle forme dell'art. 11, comma 1, del D.lgs. n. 11/2010.
8. - La richiesta di rimborso delle spese di assistenza professionale non può essere accolta, alla luce delle indicazioni contenute nelle decisioni del Collegio di Coordinamento n. 3498/2012, n. 6167/14 e n. 4618/2016. In particolare, nel caso di spece difetta ogni allegazione (fattura e/o notula del professionista) utile a valutare il pregiudizio subìto.

P. Q. M.

Il Collegio – in parziale accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 1.012,95 (…omissis…)