Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) GRECO	Membro designato dalla Banca d'Italia
(RM) SCIUTO	Membro designato dalla Banca d'Italia
(RM) GRANATA	Membro di designazione rappresentativa degli intermediari
(RM) CESARO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - SCIUTO MAURIZIO

Seduta del 30/04/2020

FATTO

1. Il ricorrente, titolare di un conto corrente acceso presso la banca convenuta e cointestato con la moglie, espone quanto segue.
   In data 8.5.2019 veniva contattato telefonicamente da un sedicente operatore dell'Ufficio prevenzione frodi dell'intermediario, il quale lo informava del fatto che risultavano delle transazioni fraudolente avvenute con la sua carta di credito e che a breve il ricorrente sarebbe stato contattato dal numero verde dell'intermediario per procedere alla messa in sicurezza del suo "on line banking", così da impedire che si perpetrassero truffe anche sul proprio conto corrente. Comunicava altresì che il servizio antifrode avrebbe provveduto al blocco della carta di credito.
   Terminata la chiamata, alle ore 14:30 circa, il ricorrente provvedeva ad attivare il servizio sms alert per la notifica delle movimentazioni della carta, abbinandola all'utenza telefonica della moglie. Alle ore 14:44, il ricorrente denunciava telefonicamente

l'accaduto alla propria filiale, il cui operatore confermava che in effetti erano state eseguite alcune transazioni fraudolente sulla carta di credito, ma che era inusuale che il servizio di "fraud alert" della banca provvedesse al blocco della carta, posto che tale azione è di esclusiva competenza dell'ente emittente, che invitava a contattare. Alle ore 14:50 il ricorrente veniva chiamato dal numero 800 xxx xxx, corrispondente al numero verde della banca; il sedicente addetto della banca gli rappresentava la necessità di resettare il suo profilo sulla app youweb e nell'occasione gli comunicava che la sua user id attuale sarebbe stata sostituita con una nuova avente numero 8013xxx (risultata successivamente riconducibile ad altra correntista di BPM, parimenti truffata) e che la password di accesso sarebbe rimasta la stessa; infine faceva presente che entro la mattina del giorno successivo avrebbe ricevuto una telefonata con le istruzioni per accedere al nuovo profilo. Nel corso di questa conversazione telefonica, l'ignoto interlocutore lo informava che, per procedere al reset, avrebbe dovuto disinstallare l'applicazione (app) dal cellulare, cosa che il ricorrente faceva.

Alle ore 14:58 il ricorrente riceveva sulla propria casella di posta elettronica la notifica che il cambio del numero di telefono era stato regolarmente acquisito al sistema. Posto che poco prima aveva attivato il servizio sms alert in relazione alla carta di credito, riteneva che l'aggiornamento comunicato riguardasse proprio la carta di credito.

Il giorno seguente, 9.5.2019, alle 10:40 il ricorrente contattava l'effettivo numero verde della banca per far seguito a quanto gli era stato comunicato il giorno precedente relativamente alla necessità di resettare il proprio user id e procedere alla sostituzione con un nuovo codice. L'operatore tuttavia lo informava che la sua utenza era stata associata un numero di telefono e una e-mail riferibili a terze persone, a lui sconosciute.

A questo punto, resosi conto dell'anomalia si recava in filiale, dove l'impiegato gli faceva presente che tra le ore 15:00 e le ore 16:00 dell'8.5.2019, erano state eseguite sul conto corrente dieci ricariche dell'importo di € 4.990,00 ciascuna, su carte postepay, per un importo complessivo di € 50.010,00 inclusi i costi delle singole operazioni. Preso atto della frode che aveva azzerato il proprio conto, sporgeva la denuncia-querela alle competenti autorità.

Nella medesima giornata l'impiegato della banca forniva al ricorrente la copia delle transazioni anomale avvenute con la propria carta di credito, da cui emergeva che si era verificata una frode per il complessivo importo di € 1.250,00. L'importo veniva successivamente stornato.

2. Tanto esposto, il ricorrente afferma che i fatti esposti denotano diversi profili di colpa grave della banca nella causazione del danno patito, sia per l'omessa custodia dei dati personali sensibili, sia per la gestione della vicenda, culminata nella consumazione della truffa a danno di parte ricorrente; d'altra parte il ricorrente non ha mai ricevuto dalla banca il messaggio sms di autorizzazione del cambio/modifica dei recapiti e-mail e del numero di telefono associato al codice cliente (user id) del medesimo; infatti tali dati non sono stati inseriti nel portale web dal ricorrente, ciò che peraltro presupponeva anche la conoscenza della user-id e della password da parte dei malfattori.

   In definitiva, la banca non avrebbe predisposto misure volte ad impedire che si perpetrasse la truffa, in un contesto nel quale quest'ultima: prima era stata avvisata dal ricorrente alle ore 14:44 dell'8 maggio che era in atto una frode alla carta di credito attraverso la telefonata effettuata, con la conseguenza che la stessa banca avrebbe potuto e dovuto attuare tutte le misure di sicurezza idonee a impedire la propagazione della frode sul conto corrente, collegato alla stessa carta; poi diede corso a ben dieci richieste consecutive di ricariche di € 4.990,00 per un totale di € 49.990,00, somma assolutamente anomala, sia per la ripetitività della richiesta di ricarica della somma di € 4.990,00, sia per il profilo del correntista.

   Tanto considerato, il ricorrente chiede il rimborso della somma di € 50.010,00, maggiorata degli interessi al tasso legale con decorrenza dall'8 maggio 2019 sino al soddisfo.

3. La banca convenuta, nelle sue controdeduzioni, espone quanto segue.

   La carta di credito è stata utilizzata dal malfattore come pretesto per carpire la fiducia del cliente: infatti i dati ad essa relativa (quali ad esempio il numero di carta, l'intermediario emittente, l'intestazione, il numero di telefono, l'indirizzo, e persino il CIV) possono verosimilmente essere stati "catturati" a seguito di operazioni precedentemente effettuate dal legittimo titolare sia in occasioni di disposizioni, che tramite pagamenti effettuati presso negozi fisici. Essendo in possesso di questi dati, il malfattore si è quindi accreditato come interlocutore qualificato nei confronti del cliente, riuscendo a carpirne la fiducia ed inducendolo a fornirgli nuovi dati, ad eseguire i comandi o lui impartiti, propedeutici al perfezionamento della truffa (come ad es. la disinstallazione della App di Home Banking dal proprio telefono).

   Nel caso esame non vi è stato un furto temporaneo di identità telefonica, con conseguente aggiramento del sistemo di autenticazione a doppio fattore; infatti se fosse stata scollegata la SIM telefonica del cliente, lo stesso non avrebbe potuto ricevere le

telefonate di cui in denuncia, perché il numero di cellulare non sarebbe più stato attivo. Inoltre parimenti esclusa è la tesi di frode perpetrata tramite l'installazione di malware nel sistema informatico del ricorrente. Vi è stata, piuttosto, una sostituzione della utenza telefonica certificata collegata all'utenza Home Banking del ricorrente, effettuata secondo i protocolli di sicurezza in uso, resa possibile, purtroppo, proprio dal comportamento attivo del ricorrente che ha fornito i dati telefonicamente al truffatore.

Infatti, in data 8.5.2019, proprio alle ore 14:50:03, mentre il ricorrente era al telefono con il malfattore (come esposto in denuncia), quest'ultimo accede all'applicazione YouWeb con nickname "axxxvxxx" e dall'area privata nella sezione "contatti >dati personali> gestione cellulari", inserisce e certifica un nuovo numero di cellulare predefinito. Al fine di confermare l'operazione, la banca inoltrava quindi un OTP via SMS al vecchio numero di cellulare certificato e predefinito 345xxx e un OTP via SMS al nuovo numero di cellulare 351xxx; in entrambi i casi il malfattore ha inserito correttamente entrambi gli OTP: il primo OTP, quindi, gli sarà stato probabilmente comunicato proprio dal ricorrente durante la prima telefonata. Dopo di che, la banca ha inoltrato una e-mail di avvenuta modifica del cellulare predefinito all'indirizzo e-mail del ricorrente, ma tale mail è stata ignorata dal ricorrente - per sua stessa ammissione - confondendola piuttosto con l'attivazione del servizio di SMS alert relativi alla carta di credito.

A questo punto, nella sezione "gestione email" il malfattore ha sostituito l'indirizzo email predefinito (del ricorrente con un nuovo indirizzo ideaxxx@xxx.it; al fine di completare l'operazione, il malfattore ha inserito un OTP inviato via email a quest'ultimo indirizzo. Successivamente, alle ore 15:01, il malfattore scaricava l'applicazione YouAPP inizia l'operazione di enrollment inserendo correttamente il codice ID e il Pin personale, di cui dunque era a conoscenza, avendo avuto accesso agli OTP inviati SMS e via mail in quanto i recapiti erano stati variati ed autorizzati.

Completata la sostituzione del cellulare certificato, tutte le informazioni ed i codici necessari al perfezionamento delle successive disposizioni di pagamento online sono state inviate a questo secondo numero telefonico. Infatti il ricorrente non ha certamente ricevuto l'OTP delle 14:57, né i seguenti, perché sono stati inviati al nuovo cellulare 351xxxx inserita dal malfattore sul profilo utente, proprio grazie alla collaborazione del ricorrente. Dunque, benché il ricorrente non lo abbia ammesso, è stato proprio lui a fornire al sedicente operatore telefonico la propria parte di credenziali, inviategli correttamente al numero di cellulare 345xxxx alle ore 14:57:26.

4. Tanto esposto, la banca resistente osserva che la vicenda descritta corrisponde alla classica fattispecie di "vhishing", nel quale i truffatori carpiscono fraudolentemente le credenziali attraverso telefonate al fine di utilizzarle successivamente nel compimento di operazioni truffaldine. Si tratta, a ben vedere, di un inescusabile errore favorito da un raggiro da parte di terzi in presenza del quale la banca non poteva, e non avrebbe potuto, offrire alcuno strumento di difesa a tutela del cliente.
   Considerati tali profili di colpa grave del ricorrente, la resistente conclude per il rigetto del ricorso.
5. Il ricorrente ha depositato repliche nelle quali ha contestato quanto dedotto dall'intermediario, sottolineando come egli, alle ore 14:44 dell'8.5.2019, avesse messo al corrente la banca che era in atto una frode ai suoi danni; tuttavia la banca non attuava le misure di sicurezza idonee a impedire la propagazione della frode non solo sulla carta di credito, ma soprattutto sul conto corrente. Le richieste consecutive di ricariche di € 4.990,00 per un totale di ben 49.900,00 €, avvenute nel giro di pochi minuti ed effettuate poco dopo un cambio dati sul profilo, sono inspiegabili oltreché incompatibili con la "skillatura" (sic) del ricorrente. Inoltre, il limite dispositivo di € 50.000,00, è del tutto ingiustificabile per un profilo di "correntista base" come quello del ricorrente; si tratta di un limite eccesivo e spropositato che non è riportato in nessuna sezione del contratto sottoscritto dal ricorrente e, quindi, mai sottoposto ed accettato dallo stesso. Si tratta quindi di un vero e proprio furto d'identità, che si verifica ogni qualvolta un'informazione individuale, relativa a una persona fisica o a un'impresa, è ottenuta in modo fraudolento da un criminale, il quale agisce con l'intento di assumerne l'identità per compiere atti illeciti. Infatti tra tutti gli accessi al profilo on line avvenuti in data 8.5.2020, sono riferibili al ricorrente solo quelli avvenuti mediante il provider YYY, come accertato dagli investigatori)e precisamente: 93.44.xxxx ore 14:24:20 - app; 93.33.xxxx ore 10:31:12 - app; 93.36.xxxxx ore 14:24:07 - app; 93.44.xxxx ore 14:27:37 - youweb); non sono invece imputabili al ricorrente tutti quegli accessi eseguiti mediante provider ZZZ, e quindi attraverso l'utenza in uso al truffatore.
   Il ricorrente non ha mai comunicato alcun dato personale a terzi; infatti questi erano già a conoscenza del criminale, il quale, per completare la truffa, è ricorso anche alla tecnica dello spoofing, che consiste nella manipolazione dei dati relativi al mittente di una chiamata per far sì che la stessa appaia provenire da un soggetto differente, rimpiazzando il numero originario con un testo alfanumerico. Dal suo canto la banca non ha fornito alcuna prova che dimostri il contrario, dovendosi ritenere, pertanto, che i

detti dati siano stati acquisiti antecedentemente da parte del criminale presso la banca, responsabile in re ipsa dell'omessa corretta custodia degli stessi. In definitiva, non può ritenersi colpevole il ricorrente, per aver confuso l'e-mail di aggiunta di un nuovo numero di telefono, ricevuta alle ore 14:58, con quella di attivazione del servizio sms alert, richiesto poco prima, trattandosi di una mail del tutto generica. Le circostanze dimostrano piuttosto la responsabilità dell'intermediario per aver omesso la corretta custodia dei dati personali del correntista, e per non aver adottato tutte le misure necessarie per evitare la consumazione della truffa.

6. La banca ha depositato ulteriori controrepliche, precisando che la truffa di cui si controverte riguarda il conto corrente e non la carta di credito, tanto è vero che quanto il ricorrente contattò la banca per sollecitare l'impiegata al controllo dei movimenti della carta, i movimenti disconosciuti vennero stornati, laddove il conto corrente, in quel momento, non presentava alcuna anomalia. Contrariamente a quanto sostenuto dal ricorrente non vi è stato "furto temporaneo di identità telefoniche"; la sostituzione dei cellulari è avvenuta nell'ambito di una attività codificata e perfettamente lecita. Se non fosse possibile procedere alla sostituzione dei cellulari sui propri profili on-line (nel rispetto di protocolli di sicurezza codificati) i clienti avrebbero come unica alternativa quella di chiudere un conto in essere per aprirne uno nuovo ogni volta che dovessero cambiare operatore telefonico o numero di cellulare. Quanto al limite posto all'operatività on-line, esso è stato introdotto successivamente dalla banca nei contratti di conto corrente e fissato ad € 50.000,00, a tutela di entrambe le parti, proprio per arginare il fenomeno delle possibili truffe. È fatta salva la possibilità di procedere on-line all'abbassamento di tale limite. Le operazioni contestate non presentavano anomalie, ma erano regolari e legittime, essendosi il ricorrente autenticato secondo tutti i protocolli di sicurezza della banca. I dati forniti al malfattore non possono invece ricadere nei doveri di custodia della banca, bensì in quelli del cliente che ne ha l'esclusivo possesso. In definitiva, risulta provata la colpa grave del ricorrente, che ragionevolmente deve avere provveduto a comunicare al malfattore, nel corso della telefonata delle 14:50 le proprie credenziali e le OTP ricevute sul proprio cellulare.
7. Il ricorrente ha quindi depositato ulteriori repliche, ponendo in evidenza che nel "Documento di sintesi del servizio telephone banking" prodotto in atti, a pag. 3, si legge che "il cliente è tenuto ad operare entro i limiti operativi assegnati dalla banca per ciascun servizio ovvero tipologia di operazione", ma non è specificato quale sia tale limite; quanto all'Allegato 2, "contratto apertura rapporti" osserva che esso reca una

data successiva alla truffa e che a firma del cliente è apposta sulla 18 pagina e le comunicazioni sui limiti di operazioni sono nelle pagine 19 e 20, sulle quali non è apposta alcuna firma.

8. La banca resistente ha, infine, depositato ulteriori controrepliche specificando che i limiti operativi dei singoli servizi, o operazioni, sono specificati nei relativi contratti, e che il limite posto all'operatività on line è fissato ad € 50.000,00, a tutela di entrambe le parti, proprio per arginare il fenomeno delle possibili truffe. È fatta salva la possibilità di procedere on line all'abbassamento di tale limite.

DIRITTO

9. Il ricorso merita un parziale accoglimento nei termini che seguono.
10. La vicenda qui considerata si inquadra nella casistica del furto di strumenti di pagamento e di identità elettronica e va pertanto valutata alla luce delle vigenti disposizioni normative in materia di servizi di pagamento, con particolare riguardo agli artt. 7, 10 e 12 del d.lgs. n. 11 del 27.1.2010 (come modificato dal d. lgs. n. 218 del 15.12.2017, di recepimento della direttiva UE 2015/2366 relativa ai servizi di pagamento nel mercato interno).
11. Tali disposizioni delineano un quadro normativo dal quale promana, in sintesi, la seguente regola di giudizio: l'intermediario che non intenda farsi carico delle perdite sofferte dal cliente per operazioni che non siano state effettivamente autorizzate, ha l'onere: (i) di provare innanzitutto di aver adottato un sistema di "autenticazione forte" per l'utilizzo degli strumenti di pagamento da parte del cliente nonché, nel caso specifico, che le operazioni siano state correttamente autenticate, registrate e contabilizzate; (ii) e poi, fornita questa preliminare prova, di provare altresì, se non il dolo, almeno la colpa grave del cliente nell'aver reso possibile il compimento delle operazioni non autorizzate; (iii) non può escludersi peraltro, provata che fosse la colpa grave del cliente, una corresponsabilità dell'intermediario per aver concorso in misura determinante alla causazione del danno per effetto di una condotta a sua volta colpevole.
12. Rispetto a questo quadro normativo, il primo elemento che, in fatto, emerge dalla complessa vicenda sopra descritta, risulta, ad avviso di questo Collegio, la grave negligenza che ha connotato la condotta di parte ricorrente.

13. La realizzazione delle dieci operazioni dedotte in lite risulta infatti essere stata possibile, per gli ignoti malfattori, innanzitutto grazie alle credenziali informatiche che parte ricorrente avrebbe dovuto mantenere riservate e che invece, incautamente, ha loro comunicato: così consentendogli di accreditare sull'home banking del ricorrente (del quale verosimilmente conoscevano già alcuni dati, spesi nella prima telefonata per accreditarsi) una nuova utenza telefonica ed un nuovo indirizzo e-mail, entrambi nella loro esclusiva disponibilità, e così di disporre le predette operazioni grazie agli OTP dispositivi necessari ad autenticarli.

14. La dinamica della vicenda occorsa, anche per come descritta dalla stessa parte ricorrente in sede di denuncia, di reclamo e di ricorso, dimostra infatti – se non altro in via di prova presuntiva - come essa sia stata vittima di un phishing avviato tramite una telefonata proveniente da un sedicente operatore dell'intermediario. Questi informava il ricorrente del fatto che erano state effettuate alcune operazioni non autorizzate con la carta di credito e che sarebbe stato contattato dal numero verde dell'intermediario per procedere alla messa in sicurezza del suo "on line banking". Il sedicente operatore contattava quindi il ricorrente, invitandolo a resettare il proprio profilo "youweb", comunicando che la sua User-Id attuale sarebbe stata sostituita da una nuova. Il ricorrente nega, per la verità, che in tale circostanza abbia comunicato i propri dati personali al sedicente operatore dell'intermediario. Tuttavia, che la rivelazione della User-ID sia avvenuta nella chiamata delle 14:50:03, pare ipotesi avvalorata dalla circostanza che proprio mentre il ricorrente era al telefono con il sedicente operatore, esattamente in quel momento qualcuno effettuava l'accesso al "YouWeb" (il servizio di home banking) con il "nickname" "axxxvxxx", cioè quello del ricorrente (come infatti risulta dalle "notifiche push inviate al device con App Sicurezza" prodotte in atti, e in particolare quella delle ore 14:55.20); e che, inoltre, pochi istanti dopo, alle ore 14:57, veniva inviato un messaggio al cellulare del ricorrente (345xxxxx, lo stesso indicato anche in sede di denuncia alle forze di polizia) contenente il primo codice OTP (776194) per consentire la modifica del nuovo numero di cellulare predefinito.

Secondo l'intermediario il ricorrente, nel corso della telefonata comunicava l'OTP al malfattore; e anche questo trova rispondenza nella circostanza che subito dopo, alle ore 14:58, veniva inviato un secondo OTP (125111) sul cellulare nr. 351xxxx – cioè quello del malfattore - proprio per confermare il cambio di utenza. Per la verità, anche al ricorrente veniva inviata, via e-mail, la conferma di avvenuta modifica del cellulare predefinito; sennonché egli - come espressamente afferma nel ricorso, ed ancora una

volta con grave negligenza - sorvolava su questo messaggio, confondendo l'operazione della quale lo si informava, relativa alla sostituzione della propria utenza telefonica certificata collegata all'Home Banking, con l'attivazione del servizio sms alert, che aveva invece effettuato la mattina.

A questo punto gli ignoti malfattori eliminavano l'indirizzo e-mail del ricorrente dalla lista contatti nell'home banking, inserendovi un nuovo indirizzo e-mail (come risulta dal report di attività versato in atti da parte resistente).

Ancora qualche minuto e finalmente i malfattori, alle ore 15:01:41, ricevevano l'OTP sms per l'attivazione (cd. "enrollment") dell'applicazione sul loro cellulare (351xxxx), inserendo correttamente il codice MQ3F9QI1 per l'attivazione del "token app" (sul punto l'intermediario ha allegato delle evidenze complete dei "log").

15. Completato tale "enrlollment", diveniva quindi agevole, per i malfattori, effettuare tutte le operazioni dedotte in lite, grazie alla conoscenza dell'user-ID, del possesso del "device" (cioè il telefono cellulare con Sim relativa alla utenza telefonica accreditata) sul quale ricevere il codice dispositivo, e del codice dispositivo stesso ("OTP") di volta in volta ricevuto e poi inserito.

16. Col che risulta pure provato – anche sulla base delle evidenze informatiche prodotte della banca resisente - come rispetto a tutte tali operazioni possa dirsi raggiunta la prova della loro corretta autenticazione, registrazione e contabilizzazione.

.*.

17. Tutto ciò rilevato, che di per sé – per quanto preliminarmente osservato, in diritto - potrebbe giustificare un rigetto del ricorso, deve però valutarsi anche – da diverso ma concorrente punto di vista – la condotta tenuta dalla banca resistente, e in particolare l'osservanza dei suoi doveri professionali di diligenza nell'aver dato diretta esecuzione a tutte le operazioni contestate.

18. Occorre rilevare, da questo punto di vista, che le operazioni furono ben dieci, anomale nel loro susseguirsi (tutte effettuate nel torno di pochi minuti), di rilevante importo sia individualmente (quasi 5.000 ciascuna) sia nel complesso (oltre 50.000 euro, comprese le commissioni): e ciò non solo in termini assoluti, ma anche in termini relativi, rispetto alle disponibilità e alla condotta consueta del ricorrente, tanto da prosciugare, di fatto, l'intera disponibilità del conto in pochissimi minuti.

19. A tale riguardo, questo Collegio (decisone n. 5550 del 21.2.2019) ha avuto modo di rilevare l'anomalia di una tale operatività che non dovrebbe passare inosservata ad un

diligente intermediario: "(…) per la verità, nella vicenda considerata, l'entità della movimentazione – non solo in termini assoluti, ma anche in rapporto all'ammontare del conto utilizzato, che venne sostanzialmente azzerato con cinque operazioni effettuate "a raffica" - sia i precedenti modelli comportamentali del cliente, avrebbero dovuto attivare un rilievo (automatico, beninteso) dell'anomalia delle operazioni fraudolente".

20. Quelle sopra evidenziate sono poi anomalie che si assommano alla ulteriore circostanza che tutte le operazioni di accreditamento delle nuove utenze collegate al sito di home banking da parte degli ignoti malfattori, nonché le successive operazioni dispositive dedotte in lite, vennero disposte – come poi accertato dalla magistratura inquirente – tramite istruzioni impartite on-line da indirizzi IP del tutto diversi, anche quanto al provider utilizzato per il collegamento, rispetto a quelli abitualmente, o almeno precedentemente, utilizzati ed ascrivibili a parte ricorrente (ed intestati piuttosto a soggetti stranieri, e in particolare extracomunitari)

21. Si tratta allora, nel complesso, di anomalie, che se certamente non può pretendersi che l'intermediario rilevi in tempo reale per mezzo di dipendenti a ciò preposti, potrebbero e dovrebbero - almeno oltre un certo limite nel quale l'anomalia si dovrebbe rivelare oltre ogni ragionevole dubbio - essere tempestivamente percepite da sistemi automatici opportunamente predisposti e tali da inibire il perfezionamento.

22. A tale riguardo vale allora ricordare come gli "Orientamenti finali sulla sicurezza dei pagamenti via internet" adottati il 19.12.2014 dall'Autorità Bancaria Europea e recepiti in Italia, nel maggio 2016, con il 16° aggiornamento della Circolare n. 285/2013, hanno esplicitato alcuni paradigmi organizzativi cui gli intermediari dovrebbero uniformarsi.
In particolare, in tema di monitoraggio delle operazioni, gli Orientamenti prevedono: (§) **10.1** "I prestatori di servizi di pagamento dovrebbero utilizzare sistemi di rilevamento e prevenzione delle frodi per individuare operazioni sospette prima che il prestatore di servizi di pagamento autorizzi da ultimo le operazioni o i mandati elettronici. Tali sistemi dovrebbero essere basati, per esempio, su regole parametrizzate (come le "Black-list" dei dati relativi alle carte compromesse o rubate) e monitorare i modelli di comportamento anomalo del cliente o del dispositivo di accesso del cliente (per esempio, un cambiamento dell'indirizzo Internet Protocol (IP) (16) o dell'intervallo IP durante la sessione dei servizi di pagamento via Internet, a volte identificati mediante controlli di geolocalizzazione IP (17), categorie di operatori commerciali online atipici per un cliente specifico o transazioni con dati anomali, ecc.)".

23. A tale riguardo, e sulla base dei predetti orientamenti, questo Collegio ha già avuto modo di rilevare che i prestatori di servizi di pagamento dovrebbero monitorare i comportamenti anomali del cliente o del dispositivo di accesso al cliente come, per esempio, un cambiamento dell'indirizzo Internet Protocol (IP) o dell'intervallo IP durante la sessione di servizi di pagamento via Internet (Coll. Roma, dec. n. 25362 del 30.11.2018 "… appare utile richiamare quanto previsto dall'art. 10 degli "Orientamenti finali sulla sicurezza dei pagamenti via internet", adottati il 19 dicembre 2014 dall'Autorità Bancaria Europea e recepiti in Italia, nel maggio 2016, con il 16° aggiornamento della Circolare n. 285/2013. La disposizione in quesitone innalza lo standard di prevenzione che deve essere garantito dall'intermediario. In particolare, i prestatori di servizi di pagamento dovrebbero monitorare i comportamenti anomali del cliente o del dispositivo di accesso al cliente (per esempio, un cambiamento dell'indirizzo Internet Protocol (IP) o dell'intervallo IP durante la sessione di servizi di pagamento via Internet)."

24. In definitiva, pare allora potersi concludere, in termini analoghi a quanto già espresso nella già sopra ricordata decisone di questo Collegio (n. 5550 del 21.2.2019) che per quanto grave sia stata la negligenza della ricorrente, senza la cui colposa cooperazione con i terzi malfattori giammai questi sarebbero riusciti ad attuare la frode subìta dalla prima, è anche vero che l'organizzazione di migliori presidi di sicurezza (quali risultano, allo stato della normativa attuale, esigibili da un intermediario secondo lo standard della sua diligenza professionale) da parte della resistente avrebbe verosimilmente, e doverosamente, potuto impedire o limitare in buona misura il compimento delle operazioni non autorizzate.

25. Ne deriva, conclusivamente, un giudizio di grave colpa dell'intermediario, seppure in concorso con quella del ricorrente, che giustifica, ai sensi dell'art. 1227, c.c., una responsabilità risarcitoria del primo verso la seconda in una proporzione prevalente che il Collegio - in via equitativa e in accoglimento della domanda subordinata della ricorrente - ritiene di stabilire nella misura di € 30.000,00.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 30.000,00.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
PIETRO SIRENA