Contributo a cura dell'avv. Francesco Dal Lago

SIM SWAP FRAUD: UNA FRODE TELEMATICA IN ASCESA.

Il nome può non dire molto, ma la cosiddetta "*SIM swap fraud*" è una frode telematica estremamente insidiosa e sempre più diffusa.

Secondo uno studio pubblicato da ABI Lab (il Centro di Ricerca e Innovazione per la Banca promosso dall'ABI) nel mese di maggio 2019, ben il 90% degli istituti di credito e operatori del settore interpellati ha dichiarato di essere stato vittima di tentativi di *SIM swap fraud* (anche se solo il 40% ha effettivamente subito un danno in conseguenza della frode).

Questa tipologia di frode si articola solitamente nei seguenti passaggi (efficacemente illustrati da ABF, Collegio di Milano, n. 25754 del 3 dicembre 2019):

- i malintenzionati acquisiscono i dati personali della vittima e le credenziali statiche (*username* e *password*) relative al suo servizio di *home banking*, tramite svariate tecniche di *hacking* (*phishing, sms spoofing*, ecc.);
- successivamente, utilizzando un documento d'identità falsificato (o rubato), chiedono al gestore telefonico la sostituzione della SIM del telefono cellulare della vittima, di modo che il numero di telefono della stessa risulti attivo sull'apparecchio telefonico dei malintenzionati;
- in tal modo, questi ultimi ottengono dal prestatore di servizi di pagamento della vittima le credenziali dinamiche (la cosiddetta OTP, *one time password*) per operare *on-line*;
- la scheda SIM del cellulare della vittima viene disabilitata poiché sostituita da quella attivata fraudolentemente, ma la serrata successione temporale delle fasi nelle quali si articola la frode spesso non consente alla vittima stessa di rilevare in tempo utile il mancato funzionamento del proprio telefono e di mettersi conseguentemente in allarme.

La prima – e tuttora unica, a quanto ci consta – pronuncia edita di un Tribunale di merito resa in un caso di *SIM swap fraud* (l'espressione in quel caso non era ancora stata utilizzata) è la sentenza del Tribunale di Roma, sez. X, del 31 agosto 2016 n. 16221 (est. Perinelli); nella fattispecie, "*la scheda sim dell'attore era stata sostituita dagli ignoti truffatori*" che avevano, al contempo, acceso (verosimilmente online) un conto corrente a nome dello stesso attore su cui avevano girocontato i fondi presenti su un "conto deposito", sempre intestato all'attore, e successivamente prelevato tali somme.

La motivazione del Giudice capitolino si fonda sul pertinente richiamo al principio generale precedentemente espresso dalla Corte di Cassazione con la sentenza del 23 maggio 2016 n. 10638 (resa in una fattispecie in cui l'attrice lamentava l'addebito sul proprio c/c di un bonifico *online* da lei mai disposto; senza, tuttavia, previa sostituzione della sim), secondo cui "*in base al rinvio all'art. 2050 c.c., operato dall'art. 15 del codice della privacy, l'istituto che svolga un'attività di tipo finanziario o in generale creditizio [...] risponde, quale titolare del trattamento di dati personali, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico del cliente mediante la captazione dei suoi codici di accesso e le conseguenti illegittime disposizioni di bonifico, se non prova che l'evento dannoso non gli è imputabile perchè discendente da trascuratezza, errore (o frode) dell'interessato o da forza maggiore.*"

Tale ricostruzione, rileva correttamente la S.C., *"è d'altronde coerente con quanto disposto pure dal D.Lgs. 27 gennaio 2010, n. 11, in ordine all'obbligo del prestatore del servizio di pagamento di assicurare che i dispostivi personalizzati forniti dai gestori non siano accessibili a soggetti diversi dal legittimo titolare.*
Anche in tal caso, in punto di ripartizione delle responsabilità derivanti dall'utilizzazione del servizio, il citato D.Lgs., artt. 10 e 11, prevede che, qualora l'utente neghi di aver autorizzato un'operazione di pagamento già effettuata, l'onere di provare la genuinità della transazione ricade essenzialmente sul prestatore del servizio. E nel contempo obbliga quest'ultimo a rifondere con sostanziale immediatezza il correntista in caso di operazione disconosciuta, tranne ove vi sia un motivato sospetto di frode, e salva naturalmente la possibilità per il prestatore di servizi di pagamento di dimostrare anche in un momento successivo che l'operazione di pagamento era stata autorizzata, con consequenziale diritto di chiedere e ottenere, in tal caso, dall'utilizzatore, la restituzione dell'importo rimborsato".

Nel nostro ordinamento la disciplina dei mezzi di pagamento è contenuta nel citato d.lgs. 27 gennaio 2010, n. 11 (modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva UE 2015/2366 relativa ai servizi di pagamento nel mercato interno, la c.d. "PSD 2", entrato in vigore il 13 gennaio 2018).

In tali disposizioni viene chiaramente tracciata, *sub* artt. 7 - 12, una precisa ripartizione degli oneri, degli obblighi e delle relative responsabilità tra prestatore del servizio di pagamento e utilizzatore dello stesso, all'insegna del principio generale del rischio di impresa a carico del primo, fatti salvi i temperamenti imposti da evidenze di specifiche e gravi violazioni delle prescrizioni comportamentali a carico dell'utilizzatore (come ricorda ABF, Collegio di Bari, n. 26914 del 31 dicembre 2019).

Ai sensi, in particolare, dell'art. 10, comma 2, del d.lgs. 27 gennaio 2010, n. 11, *"Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita [...] È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente*".

Sul richiamo a tale previsione normativa si è incentrata tutta la successiva giurisprudenza dell'Arbitro Bancario Finanziario, sistema di risoluzione alternativa delle controversie (ADR) preferito negli ultimi anni dai risparmiatori per l'economicità, la celerità della procedura e la preparazione tecnica degli arbitri.

Con la pronuncia n. 20551 del 4 settembre 2019 il Collegio di Roma ha solo parzialmente accolto il ricorso presentato dal correntista osservando *"che l'intermediario resistente ha basato il proprio sistema di autenticazione dinamico sull'utilizzo di una carta SIM, il cui possesso non può essere univocamente attribuito al titolare del conto corrente. Come dimostra il caso del presente ricorso, è infatti possibile che ignoti truffatori si sostituiscano al titolare del contratto telefonico e si approprino della carta SIM e dell'utenza utilizzata per l'autenticazione dinamica. La responsabilità di simili eventi non può essere attribuita al cliente dei servizi bancari, ma rientra nel rischio d'impresa di un intermediario finanziario, che può prevedere meccanismi aggiuntivi di verifica dell'identità del cliente nel caso di richiesta della sostituzione della carta SIM utilizzata per l'autenticazione dinamica dei clienti*"; dall'altro lato osserva il Collegio che *"il frodatore conosceva informazioni anagrafiche del ricorrente ulteriori rispetto al numero telefonico. Appare quindi plausibile che l'ignoto truffatore abbia raccolto informazioni*

riservate relative al ricorrente, incluso il codice cliente e la password per i servizi bancari online, attraverso mezzi diversi dall'accesso al suo conto bancario".

In definitiva, per il Collegio i fatti oggetto del ricorso erano "*da attribuirsi a un concorso di responsabilità del ricorrente, che non ha custodito con la dovuta attenzione il proprio codice identificativo e la propria password personalizzata statica, e, in misura prevalente, dell'intermediario resistente, che ha omesso di cautelarsi di fronte alla possibilità che la carta SIM utilizzata per l'autenticazione dinamica possa essere sostituita fraudolentemente, così vanificando i presidi di sicurezza predisposti a tutela della clientela*".

Meglio argomentate e più convincenti appaiono le pronunce successive.

Su tutte, quella del Collegio di Milano n. 25754 del 3 dicembre 2019 la quale – dopo aver ben ricordato il quadro normativo di riferimento ed aver fornito la descrizione, sopra riportata, dei passaggi attraverso cui si articola la *SIM swap fraud* – espressamente esclude "*una necessaria ed automatica corrispondenza biunivoca tra il sistema di autenticazione a due fattori adottato dall'intermediario*" (ai sensi della già citata "PSD 2") "*e una colpa grave del ricorrente*" e ciò sulla scorta della decisione del Collegio di Coordinamento dell'ABF n. 22745 del 10 ottobre 2019 che aveva chiarito (in un caso non di *sim swap fraud*, bensì genericamente di bonifici *online* disconosciuti dal correntista) che la "cattura" dei codici ben potrebbe avvenire ad opera di terzi anche in presenza di un comportamento diligente da parte del cliente (dovendosi, pertanto, escludere ogni responsabilità a carico di quest'ultimo nel caso di una aggressione informatica operata attraverso un *malware* particolarmente sofisticato, "*capace di sorprendere la buona fede anche di un pur attento fruitore del servizio*" e tale, quindi, da escludere ogni sua colpa).

In considerazione di quanto sopra il Collegio milanese ha ritenuto, pertanto, di non poter ravvisare una colpa grave dell'utente "*il quale viene invece considerato vittima di un raggiro*" – la *SIM swap fraud*, appunto – "*perpetrato con strumenti tecnologici particolarmente sofisticati*".

Anche in quel caso, tuttavia, il Collegio aveva accolto solo parzialmente il ricorso, riconoscendo il diritto del correntista ad essere tenuto indenne dal pregiudizio subito solo per le prime due operazioni fraudolente e non anche per le successive tre, disposte in pari data "*ma a diverse ore di distanza dalle prime due*" e che, pertanto, "*devono addebitarsi alla condotta gravemente colposa del ricorrente, il quale, benché abbia ricevuto attorno alle ore 17:00 dello stesso giorno un SMS relativo ad un'operazione di ricarica da lui mai richiesta e, poco dopo, abbia notato che la propria SIM risultava disabilitata, si è limitato a chiedere al proprio gestore telefonico la riattivazione della SIM e lo ha fatto solo due giorni dopo [...], ma non si è peritato di verificare se con la sua carta di pagamento erano state eseguite operazioni non autorizzate*".

Le ultime due decisioni pubblicate in tema di *SIM swap fraud* hanno pienamente accolto i ricorsi dei clienti.

Con la decisione n. 26914 del 31 dicembre 2019 il Collegio di Bari ha ritenuto "*Dirimente [...] la mancata prova, da parte dell'intermediario, della colpa grave del ricorrente*".

Da ultimo, con la decisione n. 2360 del 13 febbraio 2020 il Collegio di Milano ha accolto il ricorso del correntista non emergendo "*indicazioni di una particolare e concreta disattenzione del ricorrente*" ed emergendo "*anzi al contrario l'impossibilità di riferire in alcun modo la frode alla parte ricorrente, la quale si è anche immediatamente ed utilmente attivata*" (per bloccare il conto).

In conclusione, può dirsi che la giurisprudenza dell'ABF è ferma nell'applicare alla fattispecie di *SIM swap fraud* la previsione dell'art. 10, comma 2, del d.lgs. 27 gennaio 2010, n. 11 e nel disporre, conseguentemente, che l'intermediario rimborsi al correntista un importo pari a quello delle operazioni di pagamento fraudolentemente effettuate, con la sola eccezione delle peculiari ipotesi in cui può configurarsi una colpa grave del ricorrente.