

“ Caro Salvagente, volevo riferirvi di quanto mi è accaduto. Ero tra gli utilizzatori soddisfatti della Postepay limitatamente a ricariche di cellulare e pagamenti di abbonamenti per qualche gioco online (niente poker o azzardo ma videogiochi piuttosto famosi) e mai utilizzata su bancomat e sempre tenuta religiosamente a casa. Dunque, prima di partire per le vacanze, mi azzardo a eseguire una ricarica di 1.000 euro.

Arriva il momento fatidico dell'esperimento. Siamo di fronte a un bancomat in Thailandia, e trionfalmente esordisco con un "provo io": inserisco, digito la cifra desiderata e mi trovo di fronte alla scritta "disponibilità insufficiente". Ipotizzo che ci sia un limite di qualche tipo e abbasso la cifra. Niente...

Provo un altro circuito bancario: ancora nulla. Inizio a preoccuparmi. Vado in un bar all'interno del centro commerciale, prendiamo un gelato e provo a pagare con la carta. Di nuovo: disponibilità insufficiente. Immaginate la mia espressione. A questo punto il terrore mi assale e approfittando della connessione internet di un parente di mia moglie mi collego al sito di Poste per vedere il residuo. Mi appare una cifra quasi incomprensibile: 9 euro e spiccioli. Controllando i movimenti appaiono magicamente 6 operazioni eseguite a distanza di 1 minuto l'una dall'altra e tutte a favore dell'ente dell'energia elettrica messicana. Totale operazioni: 952,17 euro.

Non sapendo più che fare compongo il numero di assistenza Poste (a pagamento dall'estero) e la signorina mi dice che devo fare denuncia, poi recarmi all'ufficio postale e compilare un modulo di disconoscimento delle operazioni. E preparare un resoconto delle operazioni evidenziando quelle fraudolente e spedire tutto per raccomandata.

Così appena tornato in Italia e fatta la denuncia alla polizia postale (qui sono subito stato accolto da un rassicurante "mi sa che lei i soldi qui non li vede più") mi reco all'ufficio postale con tutta la documentazione.

L'esito delle indagini delle poste mi arriva il 30 maggio con la frase che temevo di leggere: "Siamo spiacenti di comunicarle di non poter procedere al rimborso". Inutile dire che non ho contatti, né sono stato in vacanza in Messico.

Come posso fare per avere indietro il maltolto, oltre che la serenità che mi ha tolto un servizio come quello di Poste con questa risposta così dal sapore di copia/incolla/spedisci senza ulteriori chiarimenti?

”

Patrizio Conz
Feltre (Belluno)

Sempre la solita storia SOLDI SPARITI dalla Po ma l'azienda fa lo

Quello raccontato dal nostro lettore è tutt'altro che un caso isolato: i ladri clonano la carta, il cliente si ritrova senza soldi e Poste rifiuta di rimborsare

Valentina Corvino

Quello che è accaduto al nostro lettore è un chiaro caso di **clonazione** della carta di credito, un furto dei codici che consentono a chi ne viene in possesso di utilizzare la carta come "meglio" crede. Non stiamo parlando di un fenomeno raro, ma di un fatto molto comune di cui chiunque è vittima potenziale, non solo gli incauti visitatori di pagine internet poco sicure: ci possono clonare la carta anche quando paghiamo gli acquisti in negozio attraverso **dispositivi POS**

La storia: la Postepay fa lo gnorri



8,6 MILIONI

le carte Postepay emesse nel 2011

+1,4 MILIONI

l'incremento rispetto al 2010

65 PER CENTO

il mercato nazionale di Postepay sul totale di prepagate

65 PER CENTO

la percentuale delle transazioni di pagamento on line

136 EURO

la media mensile di spesa per singolo cliente

o quando ci rechiamo a uno **sportello automatico** (ATM). On line è un fiorire di siti che illustrano tecniche per clonare le carte di credito.

Un furto, dunque, per il quale dovrebbe valere lo stesso principio che vale in altri casi: se depositiamo gioielli in una cassetta di sicurezza (i soldi sulla Postepay) e dopo 5 giorni non ci sono più (se ci prelevano i soldi dalla carta), l'istituto che custodisce la cassetta ci "deve" risarcire. Con **Poste Italiane** è d'obbligo il con-

dizionale perché, come scrive il nostro lettore - ma i forum di discussione on line sono pieni di racconti analoghi - alla richiesta di risarcimento accompagnata da prove certe e inconfutabili Poste risponde picche.

"Colpa sua"

Come mai? Al nostro lettore, Poste ha risposto così: "Il sito su cui è stato fatto il pagamento Postepay (quello messicano, ndr) è **sicuro** in quanto il gestore del servizio partecipa ai protocolli '3D Secure'. E tale

circostanza impedisce di intraprendere qualunque azione verso la banca dove è stata fatta la transazione".

Dunque, secondo Poste, la clonazione potrebbe addirittura **non essere avvenuta**, visto che "sono stati correttamente usati i dati in Suo unico possesso per eseguire tali operazioni". Una risposta disarmante di cui abbiamo chiesto conto all'azienda che ha preferito non commentare. È lecito sospettare - per lo meno dalla lunga serie di lamen-

Sempre la solita storia: soldi spariti...

tele che circolano in casi simili - che la risposta sia la stessa per tutti.

Cosa significa dire che il sito è sicuro, se il possessore della carta sostiene di non averlo mai visitato, di non essere mai stato in vacanza in Messico e di non avere nessuna necessità di effettuare pagamenti al gestore dell'energia elettrica messicano? Quanto vale il disconoscimento delle operazioni fatto dal titolare della carta? Quella di Poste sembra davvero una risposta **copiata e incollata**. Come dire, una scelta aziendale che nega l'evidenza.

Tenuti al rimborso

Eppure, ci ha spiegato l'avvocato **Claudia Piroso** che ha seguito legalmente molte vittime di casi come questo, Poste Italiane in qualità di "depositaria a titolo oneroso" è **tenuta al rimborso** di tutte le somme illecitamente prelevate, anche se sostiene di non essere responsabile e di aver adottato tutte le misure necessarie per evitare il verificarsi della frode.

Anche per le clonazioni del bancomat **Postamat** vale lo stesso principio. A Poste è, infatti, richiesta una particolare diligenza, superiore alla diligenza media, svolgendo attività professionale.

L'azienda, tuttavia, va dritta sulla sua strada e non intende mollare neppure di fronte alle pressioni delle associazioni dei consumatori, che più volte l'hanno sollecitata a cambiare direzione e a garantire il risarcimento, e alle pronunce dell'**Arbitro** bancario e finanziario che vanno nella direzione auspicata dai risparmiatori.



PICCIOLINI: L'ARBITRO BANCARIO DÀ RAGIONE ALL'UTENTE

"Non vi rassegnate, si può avere giustizia"

I consumatori più caparbi, quelli che vanno fino in fondo alla storia anche a fronte di un danno di piccola entità, ottengono **giustizia**.

"L'Arbitro bancario e finanziario ha sempre ritenuto Poste **responsabile** della clonazione delle carte di credito perché non esiste un sistema sicuro al 100%, come tenta di farci credere l'azienda", ci spiega **Fabio Picciolini**, di Adiconsum. "La mano criminale arriva sempre prima dell'istituto, che solo di fronte all'attacco pone rimedio rafforzando il sistema".

Picciolini, non è che è un atteggiamento comune all'intero settore? Come si comportano le banche in questi casi?

Sono un po' meno peggio. Ma anche loro non fanno salti di gioia davanti alle richieste di rimborso.

E il consumatore come può difendersi?

Il fenomeno è in costante crescita e i consumatori devono prestare sempre maggiore attenzione.

Quando si eseguano pagamenti on line con la carta di credito è importante avere un buon browser di protezione, in grado di individuare i link sospetti. Ed è bene porre attenzione a tutte le e-mail "ambigue" in cui vengono richiesti i dati di home banking e i codici personali, perché proprio attraverso queste richieste i frodatori informatici riescono a clonare le carte di credito. Chi paga abitualmente con carte di credito deve cercare di coprire la tastiera mentre digita il codice e dopo l'acquisto non deve buttare lo scontrino, perché i clonatori con la tecnica del "trashing", ossia frugando nella spazzatura, possono risalire alla matrice. È buona norma, infine, conservare gli scontrini fino a che la spesa non viene visualizzata sull'estratto conto, che deve essere fatto con una certa regolarità. Ancora: mentre effettuiamo un prelievo con il Bancomat, badiamo a eventuali presenze sospette, di persone o dispositivi. ■