

# Transazioni fraudolenti con carta di credito a seguito di un attacco di phishing

Oggetto: **Abuso e truffa**      Numero del caso: **2023/07**

Il cliente contestava diverse transazioni dell'importo complessivo di 12'000 franchi, attribuite alla sua carta di credito. Il cliente era stato vittima di un attacco di phishing durante il quale aveva inserito in un sito web di phishing i dati della sua carta e un codice di conferma. La comunicazione di questi dati da parte del cliente ha permesso ai truffatori di registrare la sua carta in un borsellino elettronico (Payment Wallet) che avevano attivato su di un dispositivo elettronico mobile in loro possesso e di eseguire le transazioni contestate. Il cliente riconosceva di aver commesso un errore. Egli rimproverava però al sistema di sorveglianza delle transazioni della banca di non aver constatato il carattere inusuale delle operazioni contestate e di non averle bloccate, nonostante con queste sia stato superato il limite di utilizzo della carta di credito. Inizialmente, la banca ha rifiutato qualsiasi gesto a favore del cliente. Poi, nell'ambito della procedura di mediazione, essa ha accettato di fare un gesto a favore del cliente in considerazione del fatto che le transazioni contestate avevano superato il limite di utilizzo. La banca ha così offerto al cliente un indennizzo di 3'000 franchi. Offerta che egli ha accettato.

Il cliente, intenzionato a fare acquisti su Internet per un importo di circa 100 franchi, si è collegato su di un sito fraudolento. In questo sito, i truffatori hanno fatto credere al cliente che, per poter effettuare il pagamento, egli doveva caricare l'importo dell'acquisto su di una carta Samsung prepagata. Dopo che il cliente aveva inserito sul sito fraudolento i dati della sua carta di credito, la banca gli aveva inviato per SMS sul suo cellulare un codice di conferma. In questo SMS era indicato che il codice serviva a effettuare una registrazione su Samsung-Pay, che il codice doveva essere inserito solo nell'applicazione Samsung Pay e che esso non doveva essere trasmesso o inserito su un sito web. Nonostante ciò, il cliente aveva inserito il codice sul sito web fraudolento, ritenendo che ciò fosse necessario per ricaricare la carta Samsung prepagata. In realtà i truffatori avevano utilizzato i dati ottenuti dal cliente per Samsung-Pay per registrare la sua carta di credito su un apparecchio in loro possesso. Dopo questa registrazione, in un secondo SMS, la banca aveva confermato al cliente che la sua carta poteva ora essere utilizzata per Samsung-Pay. Il cliente era quindi convinto di aver ricaricato correttamente la carta prepagata Samsung. In realtà, i truffatori erano ora in grado di utilizzare la sua carta tramite il dispositivo mobile a loro disposizione. Essi hanno quindi fatto acquisti, senza che il cliente lo constataste, poiché le transazioni venivano confermate nell'app installata sul dispositivo elettronico mobile utilizzato dai truffatori.

Le transazioni contestate sono state effettuate per la maggior parte lo stesso giorno, a brevi intervalli e per importi considerevoli, in un negozio di abbigliamento e in un negozio di elettronica, entrambi situati all'estero. Da quanto indicato dal cliente, queste transazioni erano inusuali sia per la loro natura che per il loro importo. L'Ombudsman ha quindi chiesto alla banca perché il sistema di sorveglianza delle transazioni non aveva identificato come fraudolenti le transazioni contestate. Secondo quanto può osservare l'Ombudsman, un sistema di sorveglianza delle frodi conforme allo stato della tecnica fa parte dello standard usuale nel settore delle carte e al giorno d'oggi può anche essere presupposto dai clienti. Tuttavia, anche questi sistemi non sono in grado di riconoscere tutti i tentativi di frode. In altre parole, il cliente non ha alcun diritto a un riconoscimento efficace della

frode.

Nella presa di posizione che la banca ha indirizzato all'Ombudsman, essa ha dapprima trattato del procedimento nell'ambito del quale la carta di credito era stata registrata nella soluzione di pagamento mobile. Essa faceva valere che, comunicando i dati della sua carta e il codice necessario per la registrazione, il cliente aveva violato i suoi obblighi di diligenza e che, in virtù delle disposizioni contrattuali relative all'utilizzo della carta, egli non poteva perciò pretendere al pagamento di un indennizzo. Secondo la banca, il cliente non aveva tenuto conto dei messaggi ch'essa gli aveva inviato tramite SMS. Se lo avesse fatto e se, tenuto conto della contraddizione tra quanto comunicato dalla banca via SMS e quanto gli avevano fatto credere i truffatori, avesse preso contatto con la stessa, la truffa avrebbe potuto essere evitata. Inoltre, il cliente avrebbe avuto la possibilità di configurare la sua carta in modo tale che ogni transazione superiore a un determinato importo gli fosse comunicata con un messaggio push sul suo telefono cellulare. Il cliente non si era però avvalso di tale possibilità. Se lo avesse fatto, avrebbe notato la truffa dopo la prima transazione. Una notifica tempestiva presso i servizi della banca avrebbe permesso di evitare ulteriori transazioni fraudolenti.

La banca ha inoltre fatto valere che, per garantire la sicurezza dei suoi clienti, essa utilizzava un moderno sistema di sorveglianza delle transazioni con lo scopo d'individuare quanto prima quelle fraudolenti. Secondo la banca l'utilizzo di un tale sistema non esonera però il titolare della carta dai suoi obblighi di diligenza. I criteri in base ai quali il sistema di sorveglianza considera sospetta una transazione dipendono da numerosi fattori. Da quanto affermato dalla banca, nel caso di specie, il sistema non aveva classificato le transazioni contestate come sospette, anche perché la carta era stata precedentemente registrata per Samsung-Pay mediante un'autenticazione a due fattori. La banca ha pure fatto valere che il cliente utilizzava regolarmente la sua carta anche per più transazioni al giorno. Le transazioni erano inoltre state effettuate in negozio e avrebbero potuto corrispondere agli acquisti tipici di un turista. La banca si è perciò dichiarata disposta a concedere al cliente unicamente un compenso di 1'500 franchi, equivalente all'importo con il quale era stato oltrepassato il limite di utilizzo della carta.

Poiché l'Ombudsman intravedeva ancora notevoli discrepanze tra il profilo d'utilizzo del cliente e le transazioni fraudolenti e non riusciva a capire in che misura gli ingenti acquisti di apparecchiature elettroniche, fatti in un luogo non proprio noti per prodotti elettronici convenienti, corrispondessero al comportamento tipico di un turista, egli ha posto alla banca domande complementari. Quest'ultima ha mantenuto la sua posizione precisando che il sistema di rilevamento delle frodi non faceva parte della convenzione contrattuale con il cliente e ch'esso non era affidabile al 100%. Secondo la banca, per ridurre al minimo gli abusi con carte di credito, sarebbe necessaria una combinazione tra il rispetto degli obblighi di diligenza da parte del cliente, misure supplementari, come l'autenticazione a due fattori, e il sistema d'individuazione delle frodi. La banca era tuttavia disposta non solo ad assumersi l'importo del superamento del limite di utilizzo, ma anche a rimborsare al cliente l'intero importo della transazione che aveva portato a tale superamento. L'indennizzo offerto al cliente è quindi stato raddoppiato a circa 3'000 franchi. L'Ombudsman ha raccomandato al cliente di accettare l'offerta della banca, ritenendo vani ulteriori sforzi di mediazione. Il cliente ha seguito questa raccomandazione.