Pagamento fraudolento con carta di credito

Oggetto: **Abuso e truffa** Numero del caso: **2020/10**

> La cliente ha ricevuto una e-mail che pensava provenisse dalla Posta e con la quale le veniva chiesto di cliccare su un link per pagare 2,99 franchi per ricevere in consegna un pacco. Siccome aspettava un pacco da Zalando, ha seguito queste istruzioni. La cliente è stata reindirizzata su un sito web, che ha scambiato per quello della Posta, dove ha inserito i dati della sua carta di credito. L'emittente della carta di credito le ha poi inviato un codice via SMS, che ha anche inserito sul sito web. Poco dopo, l'emittente della carta di credito le ha inviato la conferma di un pagamento di 1'500 CHF. La cliente ha immediatamente contattato l'emittente della carta di credito. Quest'ultima ha chiarito l'incidente ma ha rifiutato di risarcire la cliente. La cliente si è quindi rivolta all'Ombudsman. Nella procedura di mediazione, l'emittente della carta di credito ha infine proposto di risarcire la cliente con 800 franchi, offerta che lei ha accettato.

Sfortunatamente, questo schema di truffa, che si rivolge principalmente ai clienti della Posta o di altri servizi di corriere, è ben noto. Con il pretesto che devono pagare una piccola tassa per ricevere un pacco, un SMS o una e-mail reindirizza i clienti verso un sito web falso, affinché vi inseriscano i dati della loro carta di credito. Questa pratica è chiamata "phishing". In realtà, con i dati rubati, i truffatori innescano un pagamento molto più alto. Nel caso in esame, sono stati addebitati 1'500 franchi alla carta di credito della cliente per pagare una fattura emessa da un'agenzia di viaggi straniera. Anche se la cliente ha scoperto e segnalato immediatamente la frode, poiché utilizzava una funzione dell'emittente della carta di credito che la informava via SMS di ogni addebito sulla sua carta, l'emittente della carta di credito non ha potuto impedire ai truffatori di effettuare la transazione resa possibile grazie ai dati della cliente. Ciò è dovuto a una regola della rete della carta di credito in questione, secondo la quale lo storno di una tale transazione in una procedura di chargeback non può essere richiesto se il titolare della carta ha autorizzato la transazione attraverso un processo di autenticazione a due fattori.

In un processo di autenticazione a due fattori, al titolare della carta viene richiesto di confermare una transazione online con carta di credito utilizzando un'applicazione o un codice inviato via SMS a un numero che ha precedentemente registrato con l'emittente della carta di credito. In alcuni sistemi di autenticazione, non viene registrato solo il numero di telefono del titolare della carta ma anche il numero dell'apparecchio ad esso collegato. Usando un tale sistema, un commerciante si protegge da una possibile richiesta di restituzione e si assicura di poter mantenere l'importo addebitato sulla carta di credito.

Nel caso specifico, le condizioni d'utilizzo della carta di credito prevedevano che l'emittente della carta di credito fosse responsabile dei danni derivanti dall'uso improprio della carta, a condizione che il cliente avesse rispettato tutti gli obblighi impostili dalle stesse (in particolare il suo dovere di diligenza) e che non avesse colpa. Secondo l'emittente della carta di credito, tuttavia, la cliente ha violato un importante obbligo di diligenza nella misura in cui ha trasmesso i dati della carta e il codice di conferma ai truffatori, e quindi a terzi sconosciuti, inserendoli sul sito web fraudolento, che aveva scambiato per quello legittimo della Posta.

In risposta all'obiezione dell'Ombudsman che la cliente ha semplicemente inserito i dati necessari per

un pagamento e non si è resa conto che il sito web era contraffatto, l'emittente della carta di credito ha dichiarato che, a suo parere, qualsiasi cliente che "abbocca" a un tale sito di phishing infrange il proprio dovere di diligenza. Sarebbe comunemente noto che non bisogna cliccare su link inviati da mittenti sconosciuti. In questo caso, l'indirizzo del mittente dell'e-mail indicava chiaramente che non era la Posta. Cliccando sull'URL del sito web, la cliente sarebbe stata anche in grado di vedere che questo era l'indirizzo dell'ufficio postale solo prima facie, con il vero indirizzo del sito di phishing che appariva sullo sfondo. Inoltre, era insolito che venissero addebitati importi non arrotondati in relazione alla consegna di pacchi. Secondo l'emittente della carta di credito, la cliente ha usato il codice di conferma inviatole per SMS, che diceva: "Il suo codice per il pagamento è: XXX". L'emittente della carta di credito ha anche fatto riferimento a un'applicazione che avrebbe potuto semplificare ulteriormente il processo di conferma. Secondo l'emittente, il fatto che né l'importo del pagamento né l'identità del fornitore di servizi apparissero nell'SMS era conforme allo standard dell'epoca. Nel frattempo, ciò era però stato cambiato, in modo che l'importo e il fornitore di servizi fossero comunicati contemporaneamente al codice richiesto.

L'Ombudsman ha chiesto all'emittente della carta di credito di riconsiderare la sua posizione. Questo perché essa richiedeva una certa conoscenza tecnica da parte della cliente, che l'Ombudsman non credeva che il pubblico in generale avesse. Inoltre, la mancanza di informazioni nell'SMS sull'importo del pagamento e sul fornitore del servizio ha contribuito significativamente al successo della truffa. Alla fine, l'emittente della carta di credito si è offerto di rimborsare alla cliente 800 franchi, ovvero poco più della metà del danno, cosa che la cliente ha accettato.