

# Frode con carta di credito in relazione a una transazione su una piattaforma di vendita online

Oggetto: **Abuso e truffa** Numero del caso: **2022/14**

La cliente aveva messo in vendita un letto su una nota piattaforma online. La cliente era poi stata contattata da una persona che si è finto interessata e che ha preteso voler trasferire l'ammontare richiesto sul conto della carta di credito della cliente tramite un servizio di pagamento gestito dalla Posta. La cliente ha quindi inserito i dati della carta di credito su un sito web falsificato che assomigliava a quello della Posta. I truffatori sono poi riusciti a utilizzare questi dati per effettuare due transazioni presso fornitori di servizi di pagamento per un totale di circa 900 franchi. Sebbene la frode sia stata scoperta immediatamente, non è stato possibile annullare gli addebiti. L'emittente della carta di credito ha rifiutato di compensare una parte del danno subito dalla cliente perché quest'ultima aveva autorizzato le transazioni con un codice inviato sul suo cellulare nell'ambito di una procedura di autenticazione detta a due fattori. A seguito dell'intervento dell'Ombudsman, l'emittente della carta di credito ha accettato di compensare la metà del danno. La cliente ha accettato questa soluzione.

Nell'anno in esame, l'Ombudsman è stato più volte confrontato a questo schema di frode. Esso è in relazione a piattaforme online molto diffuse. I truffatori inducono le loro vittime a inserire i dati della loro carta di credito su un falso sito web della Posta, facendo credere loro che in questo modo riceveranno in modo sicuro sul conto della loro carta di credito il pagamento dell'oggetto che hanno messo in vendita. I truffatori utilizzano poi i dati, ottenuti in modo fraudolento, per effettuare transazioni a carico della relativa carta di credito.

Nel caso di specie, durante la chat la cliente ha scambiato con una persona che ha fatto finta voler assisterla. Dopo aver inserito i dati della carta di credito sul falso sito web, questa persona ha detto alla cliente che avrebbe ricevuto un codice sul cellulare che le sarebbe servito a finalizzare il pagamento del letto che aveva messo in vendita. In realtà, si trattava del codice che l'emittente della carta di credito aveva inviato via SMS al cellulare della cliente per autorizzare l'addebito sulla carta di credito della transazione che i truffatori avevano effettuato con i dati ricevuti. Il presunto assistente ha poi finto che il trasferimento del prezzo d'acquisto non fosse andato a buon fine e ha chiesto più volte alla cliente di inserire i diversi codici che ella riceveva. In realtà, procedendo in questo modo, i truffatori hanno cercato di effettuare più transazioni abusive a carico della carta di credito della cliente.

Gli SMS con i codici di autorizzazione ben indicavano che si trattava di addebiti e non di accrediti. In considerazione della valuta indicata era pure chiaro che essi non avevano nulla a che fare con il pagamento promesso a favore della cliente. Nonostante quest'ultima abbia posto domande critiche e abbia rifiutato di trasmettere diversi codici che aveva ricevuto, ella è stata talmente manipolata e messa sotto pressione dai truffatori che ha inviato loro il codice d'autorizzazione per due transazioni. Procedendo in questo modo, la cliente ha autorizzato che alla sua carta di credito venisse addebitato un totale di circa 900 franchi da parte di due fornitori di servizi di pagamento internazionali. Durante la procedura di autorizzazione, la cliente ha consultato l'app della sua carta di credito e si è subito resa conto di essere stata vittima di una frode. Ha contattato immediatamente l'emittente della carta di credito, che ha bloccato la carta.

Con riferimento alle condizioni contrattuali per l'utilizzo della carta di credito, l'emittente si è rifiutata di rimborsare alla cliente le transazioni effettuate a suo scapito in modo fraudolento. Essa ha motivato la sua posizione con il fatto che la cliente le aveva confermate nel contesto della cosiddetta autenticazione a due fattori, ossia trasmettendo i codici inviati sul suo telefono cellulare. La cliente ha quindi sottoposto il caso all'Ombudsman. Era angosciata perché, a suo dire, era una madre single che viveva in condizioni molto modeste e il danno subito rappresentava un grande onere per lei.

L'Ombudsman ha contattato l'emittente della carta di credito e ha chiesto dei chiarimenti sull'esatta procedura di addebito e sulla procedura di autenticazione. Egli ha inoltre chiesto delle spiegazioni complementari sulle disposizioni contrattuali in base alle quali essa aveva rifiutato di rimborsare la cliente. Infine, ha chiesto all'emittente della carta di credito se avesse tentato di recuperare presso i fornitori di servizi di pagamento gli importi che erano stati trasferiti loro, in modo che questi potessero bloccare l'ulteriore trasferimento del denaro. Secondo quanto osservato dall'Ombudsman, ciò è consuetudine nelle operazioni di pagamento quando viene segnalata una frode.

Nella sua risposta all'Ombudsman, l'emittente della carta di credito ha spiegato in dettaglio il processo di transazione e la procedura di autenticazione dal suo punto di vista e ha affermato che le condizioni d'utilizzo della carta escludevano qualsiasi indennizzo nel caso in cui i dati della carta e il codice per l'autorizzazione della transazione erano stati divulgati a terzi non autorizzati. Inoltre, qualsiasi responsabilità dell'emittente era generalmente esclusa se le transazioni venivano confermate dal cliente nell'ambito di un'autenticazione a due fattori, come nel caso in questione. L'emittente della carta ha anche messo in risalto gli avvertimenti pubblicati sul suo sito web come pure sulla piattaforma di vendita online in questione contro il rischio di phishing.

Infine, l'emittente ha sostenuto che, a differenza di un bonifico bancario, una transazione con carta di credito non può in linea di principio essere annullata dopo che è stata autorizzata tramite l'autenticazione a due fattori, anche se l'illegalità viene accertata subito dopo. In rari casi, gli esercenti stornano la transazione se la merce non è ancora stata consegnata o il servizio pagato con la carta non è ancora stato fornito. Queste condizioni non erano state soddisfatte nel caso in questione. Nella sua risposta, l'emittente non si è invece espresso sulla questione se essa avesse almeno tentato di contattare i prestatori di servizi di pagamento a favore dei quali erano state fatte le transazioni fraudolenti.

Dopo che l'Ombudsman è intervenuto una seconda volta e ha discusso il caso con l'emittente, quest'ultima ha infine accettato di rimborsare alla cliente il 50% della perdita come gesto commerciale e senza riconoscere alcun obbligo legale. L'Ombudsman ha spiegato alla cliente gli argomenti che l'emittente gli aveva presentato e le ha raccomandato di accettare la sua offerta, ritendendola adeguata date le circostanze del caso. La cliente ha accettato l'offerta.