Registrazione fraudolenta di una carta di credito in un portafoglio elettronico (come Apple Pay o Samsung Pay)

Oggetto: **Abuso e truffa** Numero del caso: **2020/11**

> In un periodo di tempo molto breve, sulla carta di credito del cliente sono stati addebitati più di 21’000 CHF, un importo superiore al suo limite di credito di 2’000 CHF. Gli addebiti provenivano da un paese scandinavo, dove il cliente non era presente in quel momento. In risposta al reclamo del cliente, l’emittente della carta di credito ha sostenuto ch’egli aveva comunicato i dati della sua carta a terzi sconosciuti, permettendo loro di memorizzare la carta in un portafoglio elettronico ed eseguire le transazioni. L’azienda si è quindi offerta di rimborsargli poco meno del 75% del danno causato dall’uso improprio della carta. Il cliente non era soddisfatto di questa offerta e si è rivolto all’Ombudsman. Nella procedura di mediazione, l’emittente della carta di credito ha accettato di aumentare la compensazione all’85%, un’offerta che il cliente ha accettato con riluttanza.

Il cliente ha spiegato all’Ombudsman che non solo è molto attento alla sua carta di credito, che usa principalmente per le transazioni online, ma protegge anche tutti i suoi dispositivi elettronici con un software di sicurezza costantemente aggiornato. Sosteneva di non aver mai comunicato i dati della sua carta di credito a terzi e non capiva come potessero essere stati fatti gli addebiti contestati. Secondo lui, tali addebiti erano molto insoliti per lui e avrebbero dovuto attirare l’attenzione dell’emittente della carta di credito, soprattutto perché superavano di molto il suo limite di credito. Aveva aumentato il suo limite di credito a CHF 19’000 durante un viaggio negli Stati Uniti e sfortunatamente aveva dimenticato di abbassarlo di nuovo a CHF 2’000, cosa che ha comunque fatto subito dopo l’incidente.

Nella sua presa di posizione all’Ombudsman, l’emittente della carta di credito non ha messo in dubbio il fatto che le transazioni contestate dal cliente siano state fatte da una terza parte non autorizzata. Tuttavia, l’uso dei dati della carta in un portafoglio elettronico è equivalente all’uso della carta con un codice PIN. I terzi non autorizzati possono usare una carta in un portafoglio elettronico solo se hanno i dati necessari della carta. Inizialmente, però, questi dati sono sempre trasmessi al solo titolare della carta. Pertanto, il fatto che una terza parte sia in grado di ottenere questi dati, compreso il codice di conferma per l’autenticazione a due fattori, è una violazione del dovere di diligenza del titolare della carta. Poiché, in ogni caso, i dati non possono essere trasmessi a terzi, se non per via del titolare della carta, non era importante come essi erano stati effettivamente trasmessi. Secondo l’emittente della carta di credito, una carta può essere conservata in un portafoglio elettronico solo dopo un processo di autenticazione a due fattori. Si deve quindi presumere che le transazioni con tale carta siano iniziate o autorizzate dal titolare della carta. Tali transazioni non sono quindi monitorate secondo le stesse regole delle transazioni non soggette all’autenticazione a due fattori.

Inoltre, l’emittente di carte di credito ha sottolineato che, purtroppo, i clienti sono spesso ingannati da e-mail o SMS falsi, che li invitano a cliccare sui link e a inserire i dati della loro carta di credito. Secondo l’emittente, è probabile che ciò sia accaduto nel caso di specie e che il cliente abbia rivelato tutti i dati necessari per registrare la sua carta in un portafoglio elettronico, ossia il numero della carta, la data di scadenza e il codice di verifica (CVC), nonché il numero di transazione (mTAN) ricevuto per confermare la registrazione.

Poiché il CVC si trova solo sul retro della carta e non è generalmente accessibile, l'emittente della carta di credito ha considerato che il cliente avesse precedentemente passato questo codice a terzi, forse nella convinzione di pagare un servizio desiderato o di partecipare a un concorso. Inoltre, i terzi non autorizzati devono aver ottenuto l'accesso al telefono cellulare del cliente o aver ricevuto il codice direttamente dal cliente. Infatti, il codice era accessibile solo sul cellulare precedentemente registrato dal cliente.

I sistemi dell'emittente della carta di credito hanno mostrato che sia l'SMS contenente il codice di attivazione che l'SMS di conferma sono stati inviati al numero di telefono indicato dal cliente. Dopo che una persona in possesso dei dati necessari ha presentato una richiesta di registrazione della carta come mezzo di pagamento in un portafoglio elettronico per smartphone, l'emittente della carta di credito ha immediatamente inviato il codice di attivazione, grazie al quale il processo di registrazione ha potuto essere concluso con successo. La conferma della registrazione è stata inviata anche via SMS al numero di telefono indicato dal cliente. Il testo tipico dei messaggi SMS ("Inserisci il codice di attivazione XXX per attivare la tua carta di credito che termina con XXXX in [Apple Pay / Samsung Pay]" e "La tua carta di credito che termina con XXXX è stata attivata con successo in [Apple Pay / Samsung Pay]") indicava chiaramente che la carta veniva attivata in un'applicazione di pagamento. Secondo l'emittente della carta di credito, l'uso fraudolento della carta, che ha avuto luogo alcuni giorni dopo, avrebbe potuto essere evitato se il cliente avesse reagito a questi messaggi SMS in tempo utile.

L'emittente della carta di credito ha inoltre sostenuto che le transazioni contestate erano transazioni "senza contatto" come definito nelle condizioni della carta, dove sono elencate come un'opzione di sostituzione della carta. Divulgando i dati della sua carta e inserendo lui stesso il codice di attivazione o passandolo a terzi, il cliente aveva violato il suo dovere di diligenza. L'emittente della carta di credito considerava quindi giustificato rifiutare di rimborsare il danno.

Infine, l'emittente della carta di credito ha notato che, a seconda dei casi, un limite di credito può essere superato a causa della conversione o dell'uso della carta all'estero. Inoltre, i limiti dei clienti a lungo termine sono gestiti con una certa flessibilità. Alla fine, a causa della loro relazione commerciale di lunga data, l'emittente della carta di credito era disposta, a titolo puramente bonale e senza riconoscere alcun obbligo legale, a risarcire il cliente per l'85% del danno subito.

L'Ombudsman ha trasmesso questa nuova offerta al cliente con i suoi commenti. Di regola, come stipulato nella maggior parte dei contratti pertinenti, le transazioni con carta di credito sono attribuite al cliente dal momento che sono state iniziate con i mezzi di legittimazione concordati. Gli emittenti delle carte di credito sono responsabili dei danni derivanti dall'uso improprio della carta solo se le transazioni sono state effettuate da terzi non autorizzati, senza che il cliente lo abbia reso possibile violando il suo dovere di diligenza.

La questione di come i truffatori in questo caso siano riusciti ad avere accesso ai dati necessari per memorizzare la carta di credito del cliente in un portafoglio elettronico doveva essere lasciata aperta nella procedura di mediazione. Secondo l'emittente della carta di credito, questo potrebbe essere successo solo con la partecipazione del cliente, che probabilmente è stato vittima di una frode e quindi ha divulgato i suoi dati. Tuttavia, il cliente ha contestato questi fatti. Come mediatore neutrale, l'Ombudsman non è abilitato a mettere in dubbio la credibilità delle parti. Pertanto, non avvia mai una procedura di amministrazione delle prove per accertare i fatti in modo vincolante, secondo regole specifiche, quando le parti presentano versioni contrastanti dei fatti. L'obiettivo della procedura di mediazione è piuttosto quello di risolvere le controversie in modo amichevole e l'Ombudsman può suggerire soluzioni sulla base delle informazioni fornite dalle parti. Tuttavia, l'Ombudsman non ha l'autorità di prendere decisioni vincolanti su fatti controversi o questioni legali, poiché tali questioni sono di competenza dei tribunali ordinari.

Poiché, nella procedura di mediazione, non è stato possibile chiarire ulteriormente l'incidente e l'emittente della carta di credito aveva già annunciato che non avrebbe accettato di compensare più dell'85% del danno, l'Ombudsman ha consigliato al cliente di accettare l'offerta fatta. A suo parere, sarebbe stato auspicabile che il processo di registrazione di una carta in un portafoglio elettronico fosse regolato più chiaramente nel contratto, in modo che il cliente fosse almeno informato in termini generali sul prodotto e sul suo funzionamento e potesse, per esempio, rifiutarsi di utilizzarlo. L'Ombudsman ha anche messo in dubbio l'adeguatezza della base contrattuale invocata dall'emittente della carta di credito a questo proposito. Questa base sembrava essere più appropriata per le transazioni individuali con la funzione senza contatto che per la registrazione di una carta in un portafoglio elettronico. Tuttavia, secondo l'emittente della carta di credito, risultava sufficientemente chiaro dall'SMS, ricevuto nel contesto dell'autenticazione a due fattori che il cliente, inserendo il codice, acconsentiva alla registrazione di una carta in un tale portafoglio elettronico. In considerazione della procedura utilizzata, le disposizioni contrattuali dettagliate applicabili al portafoglio elettronico erano visibili solo ai criminali sul dispositivo dal quale la carta era stata registrata, cosa che l'Ombudsman ha considerato tutt'altro che ottimale.

Dopo aver soppesato i pro e i contro dell'accordo proposto, il cliente ha finalmente accettato, anche se ha espresso la sua insoddisfazione per la gestione del suo reclamo da parte dell'emittente della carta di credito.