Betrügerische Kreditkartentransaktionen nach einem Phishing-Angriff

Thema: **Missbrauch und Betrug** Fallnummer: **2023/07**

Der Kunde beanstandete diverse Kreditkartentransaktionen in der Gesamthöhe von CHF 12 000. Es stellte sich heraus, dass er Opfer eines Phishing-Angriffs worden war, bei welchem er seine Kartendaten und einen Bestätigungscode in einer Phishing-Website eingegeben hatte. Dies ermöglichte den Tätern, die Karte des Kunden in einem Payment-Wallet auf einem fremden Mobilgerät zu registrieren und die beanstandeten Transaktionen auszuführen. Der Kunde sah ein, dass er damit einen Fehler gemacht hatte, beanstandete aber, dass das Transaktionsüberwachungssystem der Bank die ungewöhnlichen Belastungen weder festgestellt noch gestoppt hatte und dadurch seine Kartenlimite sogar überschritten wurde. Die Bank lehnte ursprünglich jede Entschädigung ab, kam ihm aber schliesslich im Ombudsverfahren wegen der Limitenüberschreitung mit CHF 3000 entgegen, was der Kunde akzeptierte.

Der Kunde wollte im Internet einen Einkauf über rund CHF 100 tätigen und gelangte auf eine betrügerische Website. Dort konnten ihm die Betrüger vorspiegeln, er müsse eine Samsung-Prepaidkarte mit dem Kaufbetrag laden, damit die Zahlung möglich sei. Er gab seine Kartendaten ein, worauf er von der Bank per SMS einen Bestätigungscode auf sein Handy zugeschickt erhielt. Auf diesem SMS war vermerkt, dass der Code für die Registrierung auf Samsung-Pay diene, nur in die Samsung Pay App eingegeben werden solle und nicht weitergegeben oder auf einer Website eingegeben werden dürfe. Der Kunde gab den Code auf der Website ein, da er glaubte, dies sei für die Ladung der Samsung-Prepaidkarte notwendig. Effektiv registrierten die Betrüger die Karte mit den erschlichenen Daten für Samsung-Pay auf einem fremden Mobilgerät. In einem zweiten SMS bestätigte die Bank dem Kunden, dass seine Karte nun für Samsung-Pay verwendet werden konnte. Er glaubte, jetzt sei die Samsung-Prepaidkarte geladen. Effektiv konnten nun die Betrüger seine Karte mit dem fremden Mobilgerät für Einkäufe nutzen, ohne dass er dies feststellte, da die Bestätigung dieser Transaktionen innerhalb der auf dem fremden Mobilgerät installierten App erfolgte.

Die beanstandeten Transaktionen fanden grösstenteils innert eines Tages in kurzen Abständen und beträchtlicher Höhe in einem Bekleidungs- und einem Elektronikgeschäft im Ausland statt. Sie waren für den Kunden gemäss seinen Angaben von der Art und der Höhe ungewöhnlich. Der Ombudsman konfrontierte die Bank deshalb mit der Frage, wieso das Betrugsüberwachungssystem die Transaktionen nicht festgestellt habe. Gemäss seiner Beobachtung gehört ein dem Stand der Technik entsprechendes Betrugsüberwachungssystem zwar zum üblichen Standard in der Kartenbranche und darf von den Kunden heutzutage wohl auch vorausgesetzt werden, aber auch diese Systeme können naturgemäss nicht alle Betrugsversuche erkennen. Mit anderen Worten besteht für den Kunden kein Anspruch auf eine erfolgreiche Betrugserkennung.

In ihrer Stellungnahme an den Ombudsman ging die Bank zuerst auf den Prozess der Kartenregistrierung in einem Payment-Wallet ein. Sie vertrat der Ansicht, der Kunde habe mit der Weitergabe seiner Kartendaten und des für die Registrierung notwendigen Codes seine Sorgfaltspflichten verletzt und deshalb auf der Grundlage der Kartenbedingungen keinen Anspruch auf eine Entschädigung. Er habe die SMS-Texte nicht beachtet. Hätte er dies getan und sich wegen der Widersprüche zwischen den Texten und dem Bild, welches die Betrüger ihm vermittelt hatten, bei

der Bank gemeldet, hätte der Betrug verhindert werden können. Zudem hätte er die Möglichkeit gehabt, seine Karte so zu konfigurieren, dass ihm jede Transaktion über einem bestimmten Mindestbetrag mit einer Push-Nachricht auf sein Mobiltelefon gemeldet werde. Diese Möglichkeit habe er nicht genutzt. Hätte er dies getan, wäre ihm der Betrug nach der ersten Transaktion aufgefallen. Bei einer rechtzeitigen Meldung hätten weitere betrügerische Transaktionen verhindert werden können.

Die Bank verwende zur Sicherheit der Kunden ein modernes Frühwarnsystem mit dem Zweck, betrügerische Transaktionen so rasch wie möglich aufzudecken. Dies entbinde jedoch den Karteninhaber nicht von seinen Sorgfaltspflichten. Nach welchen Kriterien das Frühwarnsystem eine Transaktion als verdächtig einstufe, hänge von vielen verschiedenen Faktoren ab. Im vorliegenden Fall habe das System die Transaktionen nicht als verdächtig eingestuft, insbesondere auch, da die Karte vorgängig mittels einer 2-Faktoren-Authentifizierung für Samsung-Pay registriert worden sei. Der Kunde benutze seine Karte regelmässig auch für mehrere Transaktionen pro Tag. Die Transaktionen hätten vor Ort stattgefunden und auch einem touristischen Einkaufsverhalten entsprechen können. Die Bank zeigte sich lediglich bereit, die Limitenüberschreitung von rund CHF 1500 zu übernehmen.

Da für den Ombudsman immer noch auffällige Diskrepanzen zwischen dem Nutzerverhalten des Kunden und den betrügerischen Transaktionen im Raum standen und er nicht nachvollziehen konnte, inwieweit die hohen Einkäufe in einem Elektronikgeschäft an einem Ort, welches nicht für günstige Elektronikware bekannt war, einem touristischen Einkaufsverhalten entsprechen sollten, stellte er der Bank Ergänzungsfragen. Diese hielt an ihrer Argumentation fest und präzisierte, das Betrugserkennungssystem sei nicht Bestandteil der vertraglichen Regelung mit dem Kunden und sei auch nicht 100% verlässlich. Um Kreditkartenmissbrauch zu minimieren, bedürfe es einer Kombination zwischen der Einhaltung der Sorgfaltspflichten durch den Kunden, zusätzliche Massnahmen wie der 2-Faktoren-Authentifizierung und dem Betrugserkennungssystem. Sie war jedoch trotzdem bereit, nicht nur den Betrag der Limitenüberschreitung zu übernehmen, sondern dem Kunden den ganzen Betrag der Transaktion zu vergüten, welche zu dieser Überschreitung geführt hatte. Die Entschädigung wurde damit auf rund CHF 3000 verdoppelt. Der Ombudsman empfahl dem Kunden die Annahme der Offerte, da er weitere Vermittlungsbemühungen als aussichtslos einstufte. Der Kunde folgte dieser Empfehlung.