



Heute widmen wir uns dem Thema Loyalty mit einem unschönen Szenario: dem Loyalty Betrug. Immerhin 90 Prozent aller heutigen Loyalty Programme sind laut einer aktuellen Studie von Comarch & Kantar von Loyalty Betrug betroffen.

Was wird eigentlich unter Betrug verstanden? Es geht um das Täuschen, Irreführen oder Hintergehen eines andern. Ziel ist es, sich einen unrechtmäßigen Vermögensvorteil zu verschaffen.

Das Erlangen von Vermögensvorteilen ist bei Loyalty Programmen ein Hauptbestandteil. Häufig werden Earn & Burn oder Statusprogramme als Mechanik genutzt. Nach dem Sammeln von Punkten, Meilen oder anderen Loyalty Währungen, folgt die Belohnung durch Einlösung in Prämien, Cash oder Vorteilen.

Natürlich zieht dies leider auch schwarze Schafe an. Für den einen oder anderen

Teilnehmer ist es verlockend zu schummeln oder gar vorsätzlich zu betrügen, um schnell an die Prämien zu kommen. Im Kern kann der Betrugsangriff auf drei Gruppen zusammengefasst werden. Technik, Mitarbeiter, Kunde.

Loyalty Betrug durch Technikeingriff

Seit Juli 2019 ist das Loyalty Programm „Priceless“ von Mastercard ausgesetzt. Hintergrund war der Eingriff von Hackern in die Datenbank. Hierbei wurden Kartendaten gestohlen und gleichzeitig auch Loyalty Punkte von Usern betrügerisch genutzt. Bis heute (Stand 05.02.2020) ist das Programm von Mastercard ausgesetzt. Sicherlich ein großer Vertrauensverlust beim Kunden, mit großem Imageschaden für das Unternehmen.

Loyalty Betrug durch Mitarbeiter

Auch das größte Bonusprogramm in Deutschland Payback hat immer wieder mit Betrügern zu tun. In dem bekanntesten Fall aus 2016, waren Mitarbeiter von einem teilnehmenden Partner die Initiatoren. Bei jedem Bonus relevanten Kauf wurde die eigene Payback Karte zur Punktegutschrift genutzt. Der Gesamtschaden belief sich auf 400.000 €.

Glücklicherweise konnten die Betrüger identifiziert und zur Rechenschaft gezogen werden. Aber auch hier ist natürlich ein immenser Imageverlust für Bonusprogramm und Partner entstanden.

Loyalty Betrug durch Kunden

Fragt man Loyalty Betreiber, egal ob stationäre oder Online Händler, sind auch Kunden unter den Betrügern. Insbesondere, wenn Punkte schnell gutgeschrieben und im Anschluss sofort in Prämien/Vorteile umgewandelt werden. Danach werden die Produkte retourniert ohne, dass die bereits ausgegebene Prämie/Vorteil zurückgegeben wird. Somit findet eine missbräuchliche Nutzung von Loyalty Punkten statt.

Die 7 häufigsten Betrugsarten und mögliche Abhilfen

1. Filialmitarbeiter sammeln Punkte auf ihrer eigenen Karte, sofern im Kassiervorgang bemerkt wird, dass der Kunde nicht am Loyalty Programm teilnimmt.

Tipps zum Schutz: Gutes Tracking aufbauen, z.B. mehr als drei Kundenbuchungen pro Tag werden angezeigt. Im System dürfen auf einer Karte nur eine Zahl x an Transaktionen pro Tag gebucht werden. Kundenkarten dürfen nicht von Mitarbeitern genutzt werden.

2. Kunden kaufen Artikel und erhalten Bonuspunkte, die sofort in Prämien umgewandelt werden. Im Anschluss werden die Artikel retourniert, jedoch die Punkte nicht im Loyaltysystem abgezogen.

Tipps zum Schutz: Bei Artikeln mit Retourenrecht werden die Punkte bis zur Rückgabefrist geblockt. Einstellungsoptionen im Loyaltysystem vorsehen. Gutes Testkonzept vor Launch aufbauen.

3. Falsche Konfiguration im Loyalty System oder bei angebundenen Systemen

Tipps zum Schutz: Testdurchlauf nach Einführung neu angelegter Loyaltykampagnen durchführen. Hierbei alle möglichen Fallszenarien erstellen, um Einstellungsfehler zu identifizieren. Regelmäßige Wiederholung der Testszenarien einplanen. Aktivitätenverlauf im Loyalty System überwachen, um einzusehen, wer die Loyalty Kampagne angelegt hat.

4. Punktebuchungen durch befreundete Filial- oder Service-Mitarbeiter

Tipps zum Schutz: Eingrenzung der berechtigten Personen, die Zugriff auf manuelle Punktebuchungen haben. Im Loyalty System eine Auditfunktion mit Warnsystem einsetzen. Jeder Mitarbeiter darf nur eine bestimmtes Aktions- bzw. Tageslimit zur manuellen Punktevergabe haben.

5. Schlupflöcher von Fehlkonfigurationen, um Punktwert oder Statuslevel zu beeinflussen

Tipps zum Schutz: Auch hier hilft es, vorab Testkonzepte zu entwickeln und ausreichende Tests durchzuführen.

6. Aneignung eines fremden Bonuskontos oder Identitätsdiebstahl

Tipps zum Schutz: Die IT immer wieder auf Einfalltore überprüfen. Am besten, automatische Zugriffsprüfungen mit Notifikationen installieren. Im Reporting Auffälligkeiten mittels vordefinierten Punktlimits setzen und regelmäßig überwachen.

7. Verwenden derselben Bonuskarte durch mehrere Personen

Tipps zum Schutz: Auch hier hilft das Reporting, um rasch Auffälligkeiten zu erkennen. Im Notfall Kundenkarten temporär sperren. Jedoch muss natürlich geklärt sein, ob diese Methode möglicherweise Teil des Programmkonzepts ist, sogenannte Pooling/Haushaltskonzepte.

Fazit

Sicherlich ist dies nur eine Auswahl an Betrugsmethoden und möglichen Abhilfeoptionen. Jedoch wird damit schon einmal ein Großteil eingedämmt. In der heutigen Zeit, mit schneller Weiterverbreitung von Nachrichten via Social Media, sind die Betrugsmethoden schnell veröffentlicht und können neben dem Wertverlust auch einen starken Imageverlust bei treuen Kunden verursachen. Bekanntlich sagt der Volksmund, Gelegenheit macht Diebe.



Über den Autor: Alexander Süßel ist seit 2007 als Digital Consultant aktiv. Die Umsetzung von Digitalisierungsprojekten in den Bereichen User Engagement, Loyalty & CRM sind seine Fokusthemen. Diese Expertise hat er u.a. bei Loyalty Prime, Wirecard, Department One, Brand Loyalty sowie Sensorberg als IT Projektleiter und Business Development Manager eingebracht.

Beitragsbild: *Stockfoto - Brian A. Jackson/Shutterstock*