Betrugserkennung in Echtzeit: ein Balanceakt

Von Ulrich Wiesner und Martin Warwick

Betrugsmanagement ist stets ein Balanceakt: Die Ablehnung zu vieler regulärer Transaktionen als potenziell betrügerisch gefährdet die Kundenbeziehung. Doch auch ein zu häufiges Nichterkennen von Betrugsfällen schadet der Reputation. Beim Umgang mit potenziellen Betrugsfällen raten die Autoren deshalb zur Berücksichtigung individueller Kundenprofile, wie sie im Marketing längst üblich sind. Die Verlagerung eines Teils der Betrugsabwehr auf den Kunden bewerten sie zweispältig: Die Kundenzufriedenheit darf nicht leiden. Red.

In Deutschland werden jährlich etwa 2,2 Milliarden Kartenzahlungen mit einem Gesamtwert von 150 Milliarden Euro getätigt. Legt man nun die branchenübliche Betrugsquote zugrunde, entsteht ein Betrugsschaden von jährlich rund 600 Millionen Euro. Schätzungsweise ließe sich mindestens die Hälfte dieser Schäden vermeiden, wenn durchgängig angemessene Maßnahmen zur Betrugserkennung ergriffen würden.

Im deutschsprachigen Raum beträgt das durchschnittliche Verhältnis zwischen Betrugsschäden und Kreditkartenumsätzen (Fraud to Sales) fast 50 Basispunkte. Bei unzureichenden Abwehrmaßnahmen kann dieser Wert auch deutlich höher liegen. Mit modernen Systemen zur Betrugserkennung, die Kartentransaktionen mit modernen Analytikverfahren in Echtzeit bewerten, lässt sich die Betrugsquote in der Regel auf etwa 20 Basispunkte reduzieren. Wenn sowohl die technischen als auch die organisatorischen Rahmenbedingungen stimmen, ist sogar ein Betrugsanteil von unter 15 Basispunkten möglich.

Hohe Trennschärfe entscheidend

Beim Erkennen von betrügerischen Kartenumsätzen kommt es vor allem auf zwei Dinge an: die Güte der Bewertung der Betrugswahrscheinlichkeit und die Geschwindigkeit, mit der die Bewertung durchgeführt wird. Im Idealfall erfolgt eine automatische Bewertung in Echtzeit, bei der unverdächtige Transaktionen automatisch genehmigt und Verdachtsfälle manuell geprüft werden.

Die Güte der Bewertung der Betrugswahrscheinlichkeit bestimmt, wie trennscharf zwischen Betrugsfällen und ordentlichen Umsätzen unterschieden werden kann.

Zum Autor

Dr. Ulrich Wiesner ist Lead Consultant bei FICO Deutschland, München. **Martin Warwick** ist Principal Consultant bei FICO, London.

- Reguläre Umsätze, die fälschlicherweise als riskant bewertet wurden, führen günstigstenfalls zu einer manuellen Prüfung und damit zu zusätzlichen operativen Kosten, beeinträchtigen bei einer Ablehnung der Transaktion aber die Kundenzufriedenheit und wirken sich negativ auf den Umsatz aus. Eine hohe Falsch-Positiv-Rate, also eine häufige falsche Klassifizierung als Betrugsverdacht, kann deshalb sowohl hohe operative Kosten verursachen als auch die Höhe der möglichen Umsätze und damit die Rentabilität beeinträchtigen.

- Wenn aufgrund mangelnder Trennschärfe bei der Bewertung eine hohe Falsch-Negativ-Rate hingenommen werden muss, also ein zu häufiges Nichterkennen von Betrugsfällen, führt dies zur Genehmigung einer entsprechend hohen Zahl von betrügerischen Transaktionen. Jeder nicht erkannte Betrugsfall verursacht monetäre Schäden und beeinträchtigt gegebenenfalls die Reputation der Bank sowie das Vertrauen des Kunden in die Sicherheit des Produktes.

Dynamische Profile

Die Geschwindigkeit der Bewertung bestimmt, wie schnell betrügerische Transaktionen verhindert werden können. In den allermeisten Fällen erfolgen sämtliche Missbrauchsversuche mit ein und derselben Karte innerhalb eines sehr kurzen

Zeitraumes: innerhalb einiger Minuten oder höchstens weniger Stunden.

Um Betrugsversuchen effektiv einen Riegel vorzuschieben und Schäden abzuwenden, müssen alle Transaktionen deshalb im Bruchteil einer Sekunde bewertet und neue Informationen in Echtzeit verarbeitet werden. Erst wenn jüngste Ereignisse mit längerfristigen Verhaltensmustern kombiniert werden, ist eine umfassende Situationsbewertung möglich. Moderne Systeme für Betrugsabwehr setzen dabei auf analytische Modelle, neuronale Netze und selbstlernende Algorithmen.

Der Abgleich von Echtzeitdaten mit dem Verhaltensmuster des jeweiligen Karteninhabers ermöglicht eine schnelle Entdeckung von Betrugsangriffen. Dabei wird zum Beispiel das Umsatzverhalten des Karteninhabers hinsichtlich der Art, Höhe und Frequenz bestimmter Transaktionen berücksichtigt. Analytische Modelle suchen nach Verhaltensänderungen und bekannten Betrugsmustern und reagieren im Verdachtsfall sofort.

Angesichts der Fülle an Daten, die für die Verarbeitung und Bewertung sämtlicher Transaktionen ausgewertet werden müssen, stoßen traditionelle datenbankgestützte Verarbeitungssysteme jedoch an ihre Grenzen. In der Betrugserkennung kommen deshalb heutzutage dynamische Profile zum Einsatz. Diese filtern die relevanten Informationen aus den Transaktionen heraus und machen Entscheidungen in Echtzeit überhaupt erst möglich.

Spagat zwischen Kundenfreundlichkeit und Risikomanagement

Systeme, die Transaktionen nicht in Echtzeit bewerten oder die in Echtzeit lediglich ein einfaches Regelwerk abarbeiten, können Verhaltensänderungen in der Kartenverwendung meist nicht sofort erkennen. Solche Systeme identifizieren Betrugsfälle erst im Nachhinein und bieten für Echtzeit-Entscheidungen nur eine schlechte Trennschärfe. Im Falle einer nachträglichen Identifikation von Betrug ist zwar eine Kartensperre zum Schutz vor künftigem Missbrauch möglich. Das Kind ist jedoch meist schon in den Brunnen gefallen: Betrüger wissen um den kritischen Faktor Zeit und heben deshalb innerhalb extrem kurzer Zeit einen möglichst hohen Betrag von den betroffenen Konten ab.

Im Kampf gegen Kartenbetrug versuchen einige Marktteilnehmer inzwischen, einen Teil der Betrugserkennung auf ihre Kunden zu verlagern. So informieren manche Banken ihre Kunden über jeden Kartenumsatz per SMS, in der Erwartung, der Kunde würde sich im Missbrauchsfall schon melden. Andere Marktteilnehmer verlangen etwa vom Karteninhaber, das Verfügungslimit im Ausland per Internetbanking selbst anzupassen.

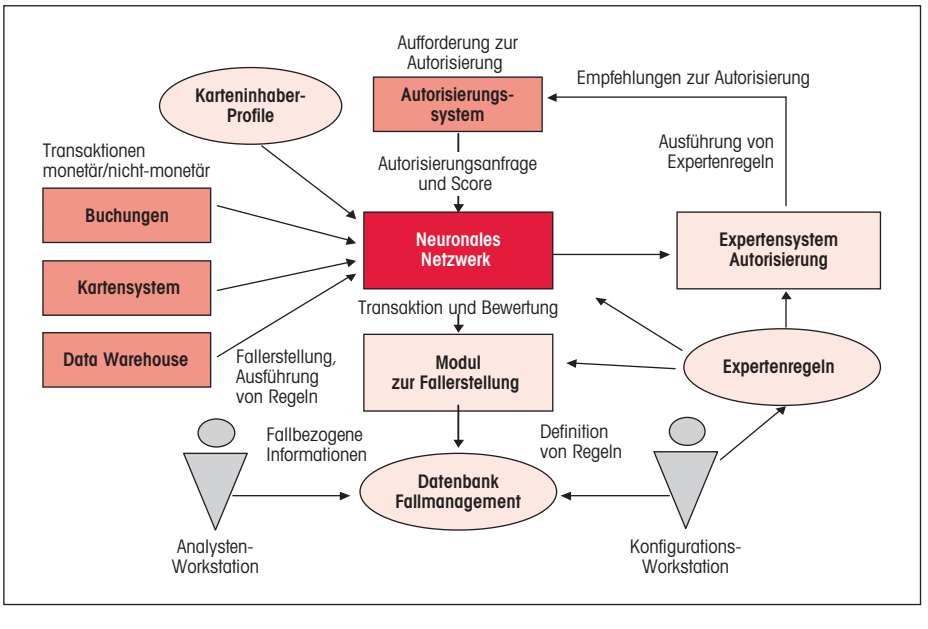
Solche Ansätze stehen im klassischen Konfliktfeld zwischen Kundenfreundlichkeit und Risikovermeidung. Kunden, die etwa im Ausland nicht über ihr Geld verfügen können, zeigen meist wenig Verständnis für solche Maßnahmen. Die Kundenbeziehung kann durch solche Ereignisse nachhaltig gestört werden.

Eine effektive Betrugsprävention erfordert ein ständiges Abwägen zwischen Betrugsvermeidung, Kundenerlebnis und operativen Kosten. Dieser Balanceakt wird auch als Fraud Appetite bezeichnet. Er definiert, in welchem Maß eine Bank bereit ist, Betrugsschäden in Kauf zu nehmen, um ihren Kunden Unannehmlichkeiten im Rahmen der Betrugsprävention zu ersparen.

Umgang mit Verdachtsfällen

Die meisten Kunden legen durchaus Wert darauf, dass ihre Bank angemessene Maßnahmen ergreift, um Betrug mit ihrer Karte zu verhindern. Sobald solche Maßnahmen allerdings den eigenen Einsatz der Karte beeinträchtigen, ist die Geduld schnell am Ende: Niemand möchte im Urlaub oder beim Einkaufsbummel feststellen, dass seine Karte nicht akzeptiert wird. Nach solchen Erlebnissen wandert die

Neuronale Netzwerke analysieren jede Transaktion, um abweichende Verhaltensmuster zu identifizieren und die Betrugswahrscheinlichkeit zu bewerten. Die Transaktion wird anschließend anhand von Scoring-Regeln genehmigt, abgelehnt oder zur manuellen Begutachtung ausgesteuert.



Karte im Portemonnaie schnell nach hinten oder wird womöglich sogar gekündigt.

Mit einem mutmaßlich betrügerischen Umsatz können Banken auf dreierlei Weise umgehen:

- Die Transaktion wird sofort abgelehnt und die Karte vorläufig gesperrt.

- Der Kunde wird um Beantwortung einer Sicherheitsabfrage gebeten, bevor die Transaktion genehmigt wird.

- Die Transaktion wird zunächst genehmigt, anschließend erfolgt eine Kontaktaufnahme mit dem Kunden, um dessen Authentizität zu überprüfen.

Mit den drei Vorgehensweisen sind unterschiedliche Risiken verbunden. Die Herausforderung besteht darin, für jede einzelne Transaktion eine individuelle Risikobewertung vorzunehmen. Dabei sind das individuelle Nutzungsverhalten des jeweiligen Kunden, das Risikoprofil der jeweiligen Akzeptanzstelle und die Art der Transaktion zu berücksichtigen. Zum Beispiel fließt in die Bewertung ein, ob die Karte physisch bei der Akzeptanzstelle vorliegt und ob der Karteneinsatz im Ausland erfolgt.

Individuelle Kundenprofile berücksichtigen

Eine Berücksichtigung des individuellen Kundenprofils ist wesentlicher Bestandteil dieses Ansatzes. So kann es zum Beispiel sinnvoll sein, eine Transaktion eines Kunden mit regelmäßigen Kartenumsätzen und regelmäßigen Zahlungseingängen trotz eines erhöhten Betrugsrisikos zu genehmigen, um die Kundenbeziehung nicht zu belasten.

Hingegen kann eine Transaktion mit denselben Merkmalen – ein Einkauf beim gleichen Händler über denselben Betrag und mit derselben Risikobewertung – abgelehnt werden, wenn es sich um einen wenig profitablen Kunden mit geringen Umsätzen handelt. Die Vermeidung eines finanziellen Schadens ist in diesem Fall höher zu bewerten als eine mögliche Beeinträchtigung der Kundenbeziehung.

In den Marketingabteilungen ist das Erstellen von Kundenprofilen und die Segmentierung von Kunden zur Unterstützung taktischer und strategischer Entscheidungen selbstverständlich. In der Betrugsbekämpfung sind Kundenprofile ein wesentlicher Bestandteil des Betrugsmanagements. Sie sollten dazu eingesetzt werden, die richtige Balance zwischen Rentabilität und Risikovermeidung herzustellen.

Betrugsmuster im Wandel

Betrugsmuster verändern sich ständig in Reaktion auf die aktuelle Marktsituation und die Fähigkeit der Kartenemittenten, bestimmte Betrugstypen zu entdecken und abzuwehren.

- So haben etwa die Einführung des Chip-PIN-Verfahrens, der zentralen Sperrdatei für das elektronische Lastschriftverfahren sowie des Systems Kuno in den vergangenen Jahren zu einer deutlichen Abnahme der Betrugsfälle mit Debitkarten geführt.

- Gleichzeitig ist eine dramatische Zunahme beim Datendiebstahl zu beobachten. Zu dieser Betrugsklasse gehört das Abfangen von Zahlungsdaten im Internet, etwa durch Trojaner, sowie das Ausspionieren von Kartendaten durch Skimming an Geldautomaten oder Zahlungsterminals und anschließende Verfügungen mit Kartendubletten im Ausland. Die in der deutschen Kriminalstatistik aufgelisteten Fallzahlen für diese Betrugsklasse haben sich in den vergangenen beiden Jahren mehr als verdreifacht, und es ist absehbar, dass bereits in diesem Jahr der Datendiebstahl die häufigste in der Kriminalstatistik erfasste Betrugsart mit Kartenbezug sein wird.

- Zudem rüsten Betrüger technisch weiter auf, übertragen an Geldautomaten abgefangene Kartendaten zunehmend drahtlos und sind nicht länger darauf angewiesen, zum Abholen der gestohlenen Daten an den Tatort zurückzukehren.

Gerade beim Skimming sind Angriffe durch organisierte Banden zu beobachten, die grenzüberschreitend arbeiten, hocheffizient vorgehen und technisch hochgerüstet sind. Sie konzentrieren ihre Angriffe auf Märkte, Marktteilnehmer und Verfahren mit dem für sie optimalen Profit-Risiko-Verhältnis und reagieren auf Abwehrmaßnahmen durch Ausweichen auf andere Finanzprodukte. Wichtig ist deshalb ein integriertes Betrugsmanagement über Produktgrenzen hinweg. Es nützt wenig, ein bereits ausgereiftes Betrugsmanagement bei einem Finanzprodukt immer weiter zu verbessern, wenn gleichzeitig bei anderen Produkten der Bank die Tore für Betrüger weit offen stehen.

Produktübergreifende Betrugsprävention

In der Betrugsprävention sind deshalb gerade solche Banken besonders erfolgreich, die ihre Betrugsprävention produktübergreifend organisieren, aktuelle Betrugsmuster ständig beobachten und die eingesetzten analytischen Modelle laufend aktualisieren.

Es ist zu erwarten, dass etwa bei einer Verbesserung der gesamtwirtschaftlichen Situation und einer damit einhergehenden Belebung der Kreditvergabe auch der Antragsbetrug zunehmen wird. Banken, die solche Entwicklungen antizipieren, können durch entsprechende Vorbereitung Angriffe auf das eigene Haus vermeiden, ohne Kompromisse hinsichtlich der Herauslage oder des in Kauf zu nehmenden Betrugsschaden machen zu müssen. Gegenüber schlecht vorbereiteten Wettbewerbern stellt dies einen erheblichen Wettbewerbsvorteil dar.