

Fachartikel

IT-gestützte Betrugsprävention

Eine steigende Zahl an Betrugsfällen beschäftigt derzeit die Finanzbranche. Die Gründe hierfür liegen vor allem in der zunehmenden Anonymisierung, Automatisierung und Internationalisierung im Geschäftsprozess. Dadurch entstehen Schlupflöcher und Lücken, die Betrüger gerne nutzen.

Erfolgreiche Betrugsversuche bedeuten für Banken und Finanzdienstleister oft enorme Vermögens- und Reputationschäden. Das Kernproblem liegt darin, dass Betrugsversuche oftmals implizit bei der Bonitätsbewertung und damit auch mit deren Methoden entlarvt werden sollen. Betrüger aber finden immer neue Lücken in dieser Prüfung, mit denen sie die Sicherheitsvorkehrungen umgehen können – ein nie endendes Hase- und Igel-Wettrennen beginnt.

Betrug von Bonität unterscheiden

Um Betrug aktiv bekämpfen zu können, ist es zunächst wichtig, dass Banken oder Finanzdienstleister bei der Antragsentscheidung zwischen Bonität und Betrug unterscheiden, also letztendlich zwischen „nicht zahlen können“ und „nicht zahlen wollen“. Entsprechend unterliegt die Betrugsprüfung auch anderen Gesetzmäßigkeiten als die der Bonität und sollte im Antragsmanagement separat adressiert werden. Betrugsfälle zeichnen sich häufig dadurch aus, dass sie im Vorfeld per se nicht auffallen, die Folge der Aktivitäten des Betrügers aber bestimmte Regelmäßigkeiten aufweist, die sich durchaus identifizieren lassen.

Unternehmen müssen unterscheiden zwischen „nicht zahlen können“ und „nicht zahlen wollen“.

So gibt es Betrüger, die ihre Daten ein wenig variieren (z.B. durch eine andere Schreibweise des Namens oder einen Zahlendreher in der Anschrift), um sich Vorteile oder Leistungen zu erschleichen. Einen weitaus größeren Schaden aber verursacht der gewerbliche Betrüger, der eine hohe Anzahl an betrügerischen Aktionen innerhalb eines kurzen Zeitraums durchführt und dadurch viel Geld erbeutet. Der Betrugsversuch ist meist gut durchgeplant – und doch weist auch er Regelmäßigkeiten auf, die sich bei den Anträgen etwa durch Auffälligkeiten bei der Adresse zeigen. Diese verschiedenen Arten von betrügerischen Verhaltensweisen gilt es zu analysieren, zu identifizieren und zu sammeln.

Mit IT-System betrügerisches Verhalten erkennen

Gerade in wettbewerbsintensiven Branchen mit großen Kundenzahlen und vielen Anträgen wie der Finanzdienstleistungs- und Telekommunikationsbranche ist es notwendig, eine Betrugsprävention einzurichten, die sekundenschnelle und dennoch sichere Entscheidungen ermöglicht. Hier empfiehlt sich eine optimale Kombination aus IT-Unterstützung und manueller Prüfung.



Autor:

Dr. Jörg Seelmann-Eggebert

Director Customer Risk und Mitglied der Geschäftsleitung bei SHS VIVEON

„Modernes Kundenrisikomanagement ist geprägt von Anonymisierung, Automatisierung und Internationalisierung. Dadurch entstehen vor allem im Antragsprozess Lücken und Schlupflöcher, die dem Betrug viele Möglichkeiten eröffnen.

Grundsätzlich folgt die Betrugserkennung anderen Gesetzmäßigkeiten als die Bonitätsprüfung. Eine Kreditentscheidung muss daher genau auf diesen zwei Dimensionen beruhen.

Die große Herausforderung besteht für Unternehmen vor allem darin, diese Dimensionen organisatorisch zu vereinen, von den Verantwortlichkeiten bis hin zu den systemischen Abläufen.“

SHS VIVEON

The Customer Management Company.

Die Basis eines optimalen Betrugserkennungssystems ist eine spezielle Datenbank, die alle bereits bearbeiteten Anträge sowie eine Blacklist speichert und fortlaufend aktualisiert.

Mit Hilfe unscharfer Suchalgorithmen und regelbasierter Mustererkennung kann das System dann automatisiert prüfen, ob es sich bei den eingehenden Anträgen um Mehrfachanträge in betrügerischer Absicht handelt.

Das wichtigste Erfolgskriterium ist hierbei die Festlegung von Suchkriterien, die möglichst viele Betrugsverhaltensmuster abdecken. So kommt es häufig vor, dass unterschiedliche Anträge bearbeitet werden, die beispielsweise alle die gleiche oder ähnliche E-Mail-Adresse aufweisen. Führt die Suche in der Datenbank zu solchen Treffern, werden diese

Fälle einem Betrugs-Sachbearbeiter zur manuellen Überprüfung vorgelegt.

Fazit: IT kann Menschen nicht ersetzen
Grundsätzlich gilt: Die Kreativität von Betrügern wird von deren krimineller Energie bestimmt. Dadurch ist die Betrugserkennung generell schwierig. Banken und Finanzdienstleister können dem „Igel“ nur auf die Schliche kommen, wenn sie ihn und sein Verhalten verstehen.

Mit diesem Wissen ist es möglich, alle eingehenden Anträge nicht nur auf Bonität, sondern separat auch auf Betrug zu prüfen. Eine IT-gestützte Lösung kann dabei helfen, Betrugsverhalten automatisch zu erkennen und auszusteuern. Aber sie kann nicht den „gesunden Menschenverstand“ ersetzen, denn durch eine automatisierte Bewertung lassen sich nur Verdachtsfälle erzeugen – die finale Prüfung obliegt letztendlich dem Menschen.

Typ	Ziel	Vorgehen
<u>Privaterschleicher</u>	Versucht, eine Leistung für sich selbst zu optimieren oder zu erschleichen.	Variation in den Daten, Inkonsistenzen in den Daten
<u>Verlegenheitsoptimierer</u>	Kunde mit bestehender Geschäftsbeziehung, der kurz- oder mittelfristige Probleme hat und diese mittels Betrug verlagern will.	Verschleierung der Daten
<u>Gewerblicher Betrüger</u>	Geschäftsmaßiger Betrüger, bei dem es um hohe Stückzahlen innerhalb eines kurzen Zeitraums geht; Der Betrugsversuch ist gut durchgeplant und weist eine hohe kriminelle Energie auf.	Immer wieder neu; meist werden nicht existente Personen und Unternehmen geschaffen.

Abb 1. Um Betrug zu erkennen, müssen Unternehmen Betrug verstehen. Unterschiedliche Betrugstypen und ihr Vorgehen.

Ihr Ansprechpartner:

Für weitere Informationen, Fragen zum Thema oder unserem Angebot wenden Sie sich an unser Customer Risk Team.

Kontakt:

T +49 89 74 72 57 - 0
F +49 89 74 72 57 - 900
Info@SHS-VIVEON.com
www.SHS-VIVEON.com

Hauptsitz:

SHS VIVEON AG
Clarita-Bernhard-Straße 27
81249 München

SHS VIVEON AG - The Customer Management Company

Die SHS VIVEON AG ist ein international agierender Business- und IT-Lösungsanbieter im Bereich Customer Management. Zusammen mit unserem Software-Tochterunternehmen GUARDEAN GmbH bieten wir Ihnen marktführende Expertise in den Bereichen Customer Value und Customer Risk Management. Unsere Kompetenzen umfassen alle Themen, die für die Umsetzung eines erfolgreichen Kundenmanagements entscheidend sind. Dazu zählen u.a. Customer Analytics, Business Intelligence und Data Warehousing.

Die SHS VIVEON AG, mit Sitz in München, ist am M:access der Börse München notiert und mit zwei Tochtergesellschaften an sechs Standorten in drei europäischen Ländern präsent: GUARDEAN GmbH (D) und SHS VIVEON Schweiz AG (CH). Mit circa 200 Mitarbeitern und mehr als 200 Kunden in 15 Ländern gehört SHS VIVEON zu Europas führenden Anbietern im Customer Management. SHS VIVEON zählt namhafte Unternehmen aus Finanzdienstleistung, Industrie, Handel und Telekommunikation zu seinen Kunden, darunter BayWa, BMW Financial Services, BP, Credit Suisse, Deutsche Telekom, Ingram Micro, RaabKarcher, o2 Deutschland, Orange, SüdLeasing und Vodafone.

Weitere Informationen zum Unternehmen: www.The-Customer-Management-Company.com