

A close-up photograph of a green leaf, showing the intricate vein structure. The leaf is positioned at the top of the frame, with a row of clear, glistening water droplets along its lower edge. The background is a soft, out-of-focus green, creating a natural and fresh aesthetic.

SHS VIVEON

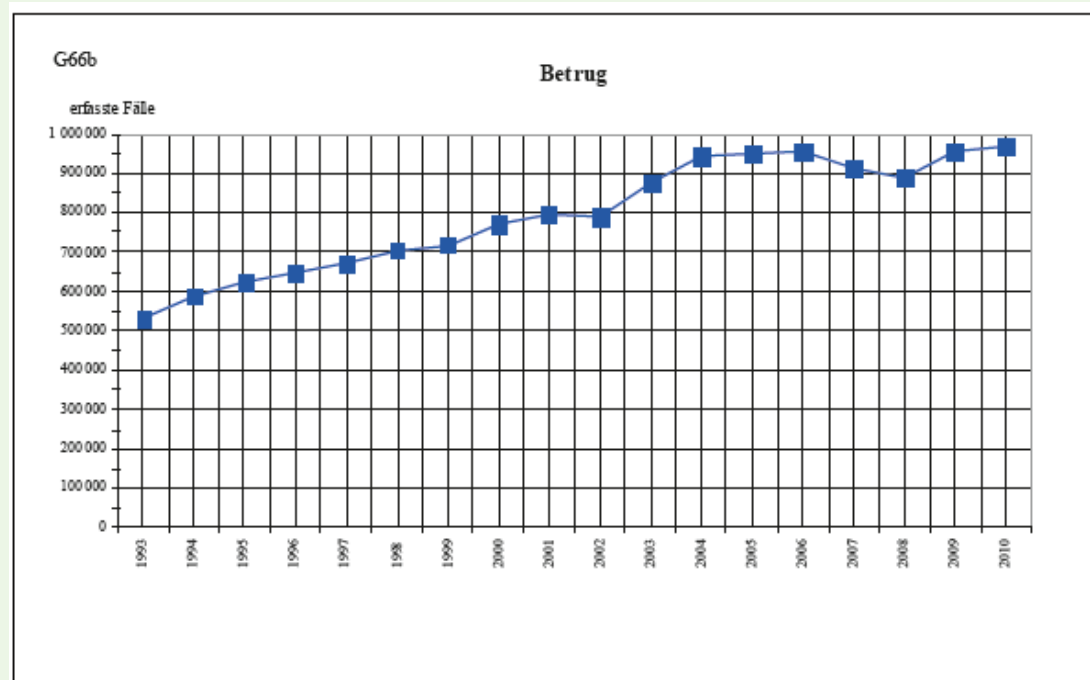
The Customer Management Company.

Betrugsprävention mit Hilfe von Risk Analytics

Steigende Zahl an Betrugsfällen

Die Polizeiliche Kriminalstatistik von 2010 zeigt: Betrug nimmt von Jahr zu Jahr immer mehr zu. Mit **968.162 Betrugsfällen** wurde 2010 die höchste Fallzahl seit Bestehen einer gesamtdeutschen Statistik im Jahr 1993 erfasst.

Betroffen ist davon zu einem Großteil vor allem auch die Finanzbranche: So verzeichnete man z.B. im Bereich **Geldwäsche einen Anstieg um 48 Prozent**.



Quelle: **Polizeiliche Kriminalstatistik 2010**,
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2011/PKS2010.pdf?__blob=publicationFile

Gesetzlich vorgeschriebene Maßnahmen zur Betrugsprävention

Der Gesetzgeber hat die Tragweite der Problematik bereits erkannt und umfangreiche regulatorische Anforderungen formuliert, die verpflichtend umgesetzt werden müssen:

GwG – Geldwäschegesetz

Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten

KWG - Gesetz über das Kreditwesen

§ 25 c KWG ab 09. März 2011

Neue Anforderungen an die internen Sicherungsmaßnahmen, insbesondere über die Einrichtung einer sog. zentralen Stelle

§ 261 StGB

Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte

Umsetzung der geforderten Betrugsprävention ist schwierig

Die gesetzlich geforderten Präventionsmaßnahmen sind komplex. Das erschwert die Umsetzung.

Eine aktuelle Befragung der SHS VIVEON AG unter Risikomanagern und Fraud-Verantwortlichen zeigte, dass bisher nur wenige Banken und Finanzdienstleister den gesetzlichen Anforderungen umfassend gerecht werden:

- So haben bislang nur etwa 70 Prozent der befragten Unternehmen die Neufassung des GWG von 2008 bereits vollständig umgesetzt und lediglich 62 Prozent erfüllen nach eigenen Angaben die Mindestanforderungen an das Risikomanagement (MARisk).
- Deutlich weniger Unternehmen, insgesamt 38 Prozent, haben sich bisher konkret mit den neu geregelten Auflagen des §25c Kreditwesengesetz (KWG) auseinandergesetzt, das am 9. März 2011 in Kraft getreten ist.



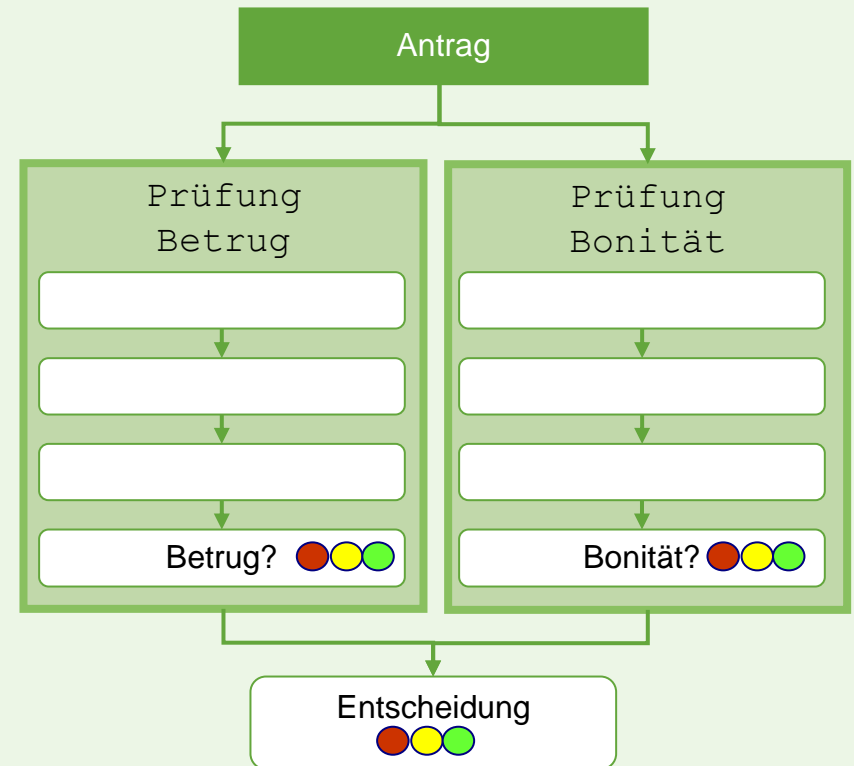
Wie können sich Unternehmen vor Betrug schützen und die vom Gesetzgeber geforderten Präventionsmaßnahmen umsetzen?

1. Schritt: Im Antragsprozess zwischen Bonität und Betrug unterscheiden.
2. Schritt: Um Betrug zu erkennen, muss man Betrug verstehen.
3. Schritt: Methoden zur Betrugsprävention im Unternehmen etablieren.

Wie können sich Unternehmen vor Betrug schützen?

1. Schritt: Im Antragsprozess zwischen Bonität und Betrug unterscheiden.

- Betrug und Bonität folgen unterschiedlichen Gesetzmäßigkeiten und adressieren damit unterschiedliche Fragestellungen:
 - Mangelnde Bonität = nicht zahlen können
 - (Antrags-)Betrug = nicht zahlen wollen
- Deshalb müssen Unternehmen die Betrugsprävention im Prüfprozess separat adressieren. Eine Betrugsprüfung sollte demnach fester Bestandteil innerhalb des Antragsmanagements werden.



Wie können sich Unternehmen vor Betrug schützen?

2. Schritt: Um Betrug zu erkennen, muss man Betrug verstehen.

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.

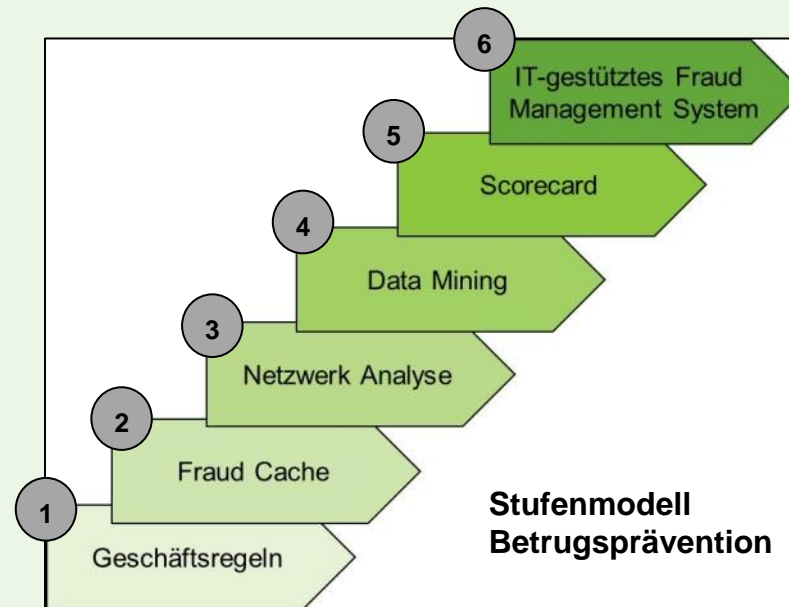
Typ	Ziel	Vorgehen
Privaterschleicher	Versucht, eine Leistung für sich selbst zu optimieren oder zu erschleichen.	Variation in den Daten, Inkonsistenzen in den Daten
Verlegenheitsoptimierer	Kunde mit bestehender Geschäftsbeziehung, der kurz- oder mittelfristige Probleme hat und diese mittels Betrug verlagern will.	Verschleierung der Daten
Gewerblicher Betrüger	Geschäftsmäßiger 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.

Die verschiedenen Arten von betrügerischen Verhaltensweisen (Privaterschleicher, Verlegenheitsoptimierer und gewerblicher Betrüger) gilt es zu analysieren, zu identifizieren und zu sammeln.

Wie können sich Unternehmen vor Betrug schützen?

3. Schritt: Methoden zur Betrugsprävention im Unternehmen etablieren.

- Bei der Erkennung von Betrugsmustern helfen unter anderem **Risk Analytics**, also statistische Analysen und Data Mining-Verfahren. Sie können neue Anträge mit Hilfe von Modellen wie etwa Scorecards bewerten und dadurch Betrugsverdachtsfälle automatisiert erkennen und aussteuern.
- In der Praxis hat sich hierbei ein **Stufenmodell** bewährt, das nach und nach umgesetzt werden kann und so die Betrugsprävention schrittweise verbessert.



Stufenmodell zur Betrugsprävention

1. Stufe: Festlegen von Geschäftsregeln

- Geschäftsregeln (Policy Rules) sind eine grundlegende Voraussetzung für den Umgang mit Betrug.
- Sie identifizieren relativ offensichtliche Betrugsverdachtsfälle, die ausgesteuert und anschließend manuell bearbeitet werden müssen.

2. Stufe: Aufbau eines Fraud-Caches

- Ein Fraud Cache ist ein Speicher etwa in Form einer täglich aktualisierten Tabelle im Data Warehouse, in dem alle Neukundenanträge eines definierten Zeitraums gesammelt werden.
- Kommt ein neuer Antrag in das System, wird der Fraud Cache auf bereits vorhandene Anträge des potenziellen Neukunden überprüft. So ist es möglich, Mehrfachanträge unter gleichen oder veränderten Identitäten zu erkennen.

3. Stufe: Etablierung einer Netzwerk-Analyse

- Ziel dieser Analyse ist es, Auffälligkeiten in Netzwerken zu entdecken.
- Es werden beispielsweise mehrfach genutzte Telefonnummern, Mailadressen oder Ausweisnummern bei unterschiedlichen Neukundenanträgen oder Bestandskundendaten gesucht.

Stufenmodell zur Betrugsprävention

4. Stufe: Einführung von Data Mining-Verfahren

- Mit Data Mining-Verfahren lassen sich gezielt Transaktionsdaten analysieren und auswerten.
- Das Ziel hierbei ist die Identifikation eines Fraud Netzwerks mit Hilfe von Kontakten bekannter Betrugsfälle zu bzw. deren Interaktionen mit anderen Kunden.

5. Stufe: Entwicklung einer Scorecard

- Scorecards liefern eine Aussage über die Betrugswahrscheinlichkeit eines neuen Antrags – diese wird dann beispielsweise auf einer sechsstufigen Rating-Skala analog dem Schulnotensystem abgebildet.
- So ist es mit Hilfe von Scorecards möglich, eine einfache, schnelle, reproduzierbare und automatisierbare Entscheidung über einen Betrugsverdacht bei Neuanträgen zu treffen.

6. Stufe: Entwicklung eines IT-gestützten Fraud Management Systems

- Die höchste Stufe im Betrugspräventions-Modell ist ein permanentes IT-gestütztes Entscheidungs- und Monitoring-System, das auf den zuvor genannten Analyseergebnissen und Scoring-Werkzeugen aufbaut.
- Durch die Einbindung interner sowie externer Daten, beispielsweise von Auskunfteien und Terrorismuslisten, können Neukunden automatisch überprüft und identifiziert und Geschäftsbeziehungen kontinuierlich überwacht werden. Dabei garantiert das System die vom Gesetz geforderte Dokumentation aller Aktionen und Daten und damit die Nachvollziehbarkeit der Entscheidungen.

Betrugsprävention durch IT-Unterstützung

Technische Systeme zur Betrugsprävention können

- die gesetzlichen Anforderungen unterstützen,
- sicherstellen, dass Prozesse immer in der gleichen Qualität und Güte ausgeführt werden,
- bei manuellen Prozessen unterstützen,
- die richtigen Daten sammeln,
- die Prozessausführung ordentlich dokumentieren,
- die interne Prüfung unterstützen,
- die „Hürde“ für Betrüger höher hängen,
- die Möglichkeit zur Spionage von Lücken schließen,

...aber nicht den gesunden Menschenverstand ersetzen.

Durch technische Systeme lassen sich nur Betrugsverdachtsmomente erzeugen, die letztendliche Prüfung obliegt immer dem Menschen.

=> IT kann Betrugsprävention unterstützen, aber nicht vollständig übernehmen.

SHS VIVEON – Ihr kompetenter Partner für Betrugsprävention

Wir helfen Ihnen bei der schrittweisen Umsetzung von Betrugspräventions-Maßnahmen, z.B.

- bei der Entwicklung von Scorecards
- bei der Implementierung eines Fraud Caches
- bei der Erkennung von Antragsmustern
- bei der Erkennung von Betrugsmustern
- bei der Identifikation der wirtschaftlich Berechtigten
- bei der Prüfung gegen Sanktionslisten
- bei der Identifizierung von Politisch Exponierten Personen (PEP)
- bei der kontinuierlichen Überwachung von Geschäftsbeziehungen
- Usw.



Ihr Ansprechpartner:

Dr. Andreas Unterreitmeier

Competence Leader Risk Analytics,
SHS VIVEON AG

KONTAKT

HEADQUARTERS

SHS VIVEON AG
Clarita-Bernhard-Str. 27
81249 München
Germany

T +49 89 74 72 57 - 0

F +49 89 74 72 57 - 900

info@SHS-VIVEON.com

www.SHS-VIVEON.com

