

**Forderungs-Management****Inkasso-Schnittstellen: Vollautomatisches Mahnwesen sichert Kleinstforderungen**

Versandhandel und klassischer Handel funktionieren nach demselben Prinzip: Ein Kauf ist ein Tauschgeschäft – Ware gegen Geld. Doch im Versandhandel ist es an der Tagesordnung, dass auf Rechnung gekaufte Ware vom Kunden nicht bezahlt wird. Bei einer Häufung solcher Fälle kann die Zahlungsfähigkeit eines Versandhauses ernsthaft Schaden nehmen.

Einen Inkasso-Dienstleister zu beauftragen, stellt deshalb eine gute Möglichkeit dar, die Liquidität nachhaltig zu sichern. Die PNO inkasso AG mit Sitz im niederbayerischen Deggendorf ist ausgesprochener Spezialist für kosteneffizientes Forderungsmanagement und automatisiertes Mahnwesen. Mit dem Einsatz innovativer Softwaretechnologien ermöglicht PNO ein völlig automatisiertes Mahnwesen und sorgt dadurch im Versandhandel für sehr hohe Kosteneffizienz.

Durch die Anbindung der ERP- und Fakturierungssysteme eines Versandhauses an die technische Infrastruktur von PNO – das umfassende Servicekonzept

von PNO basiert auf dem etablierten und weitverbreiteten .NET-Framework – können Rechnungsstellung und Mahnwesen automatisch weitergeleitet und abgewickelt werden. Zuverlässige 128-Bit-verschlüsselte SSL-Schnittstellen (.NET, XML usw.) sorgen für maximale Sicherheit bei der Datenübertragung.

**Schnittstellen vereinfachen Übergabe und Kontrolle**

Online-Versandhändlern bietet PNO inkasso besonders benutzerfreundliche Services: Über bidirektionale Schnittstellen beispielsweise zu actindo ERP und Magento können Shop-Betreiber ihr Mahnwesen direkt an PNO übergeben. Damit sparen sie sich ein aufwändiges, zeit- und personalintensives Mahnverfahren und erhöhen gleichzeitig ihre Mahnerfolge deutlich – auch bei Kleinstforderungen.

Online-Versandhändler, die das actindo ERP-System nutzen, haben die Möglichkeit, die Übernahme des Forderungsmanagements durch PNO als eigene

Mahnstufe zu definieren und vollautomatisch an PNO zu übergeben. Alternativ kann die Weitergabe des Mahnprozesses zu einem frei definierbaren Zeitpunkt mit einem Mausklick direkt aus actindo heraus erfolgen. Gleiches gilt für die Inkasso-Schnittstelle zur preisgekrönten Open Source E-Commerce-Plattform Magento: Die Übergabe ausstehender Rechnungen an PNO erfolgt entweder manuell oder automatisiert.

Bei der manuellen Übergabe markiert der Administrator in der Rechnungsübersicht eine oder mehrere ausstehende Rechnungen zur Übergabe per Mausklick. Während sich in der Administrationsoberfläche manuell festlegen lässt, zu welchem Zeitpunkt die Übergabe geschehen soll, erfolgt bei der automatisierten Task-Planung zu individuell definierten Zeitpunkten eine regelmäßige Überprüfung, ob und wie viele Rechnungen noch offen sind und an PNO übergeben werden sollen.

Über die bidirektionalen Schnittstellen zu actindo ERP und Magento können Online-Versandhändler zudem jederzeit den

Status des Mahnprozesses bei PNO in Echtzeit verfolgen.

Mit den IT-basierten Services von PNO bleiben Versandhändler zeitnah an ihren Forderungen und müssen Mahnprozesse nicht mehr aufwändig von Hand durchführen.

Die Prozess-Automatisierung steigert die Chance auf ein gutes Ergebnis: Je kürzer die Mahnintervalle, desto größer der Mahnerfolg. Kleinere Versandhändler, denen die Einrichtung einer Schnittstelle zu kostspielig ist, können ihre Forderungen auch online an PNO weitergeben. Über den Mandanten-Login erhalten alle Kunden auf der PNO-Website [www.pno-inkasso.de](http://www.pno-inkasso.de) Zugriff auf ihre individuelle Aktenübersicht, die den minutengenauen Status aller offenen Forderungsakten abbildet.

Auf sein gutes Geld verzichten – das muss heute kein Versandhändler mehr, selbst bei Kleinstforderungen.

**IT-gestützte Fraud Prevention schützt nach Maß**

Händler, die ihre Waren über das Internet anbieten, kennen die Situation. Kunden haben sich für Produkte aus dem Shop entschieden und werden nun zur Kasse gebeten. Im Bestellformular gibt der Konsument aber nur eine Handynummer an. Oder der Wert des Warenkorbes ist deutlich höher als bei anderen Bestellungen. Beide Transaktionen scheinen verdächtig – doch liegt hier tatsächlich ein Betrugsversuch vor?

Nicht wenige Online-Händler setzen an dieser Stelle auf ihr Bauchgefühl: Sie entscheiden im Einzelfall, ob sie eine Transaktion zulassen oder nicht. Diese Vorgehensweise ist aber nicht nur zeitaufwendig, sondern auch riskant: Unter Umständen wird ein möglicher Betrug nicht erkannt oder gültige Transaktionen werden fälschlicherweise abgelehnt. Die Folge: Nicht nur der aktuelle Umsatz ist verloren, der abgewiesene Kunde wird mit großer Wahrscheinlichkeit nicht wiederkommen.

Innovative IT-Lösungen, die in Echtzeit jede einzelne Transaktion überprüfen und stets die aktuellsten Betrugsmuster berücksichtigen, lösen daher zunehmend die manuelle Überprüfung ab. Sie sind die weitaus effizientere und sicherere Maßnahme, um vor Betrug zu schützen.

**Betrugsprävention in der Praxis**

Betrugsfälle zu identifizieren, ehe beim Händler ein Schaden entstanden ist, gehört zu den Hauptanforderungen an IT-gestützte Fraud Prevention. Gleichzeitig soll auch die Anzahl der Falsch Positiven, also der fälschlicherweise als Betrug gekennzeichneten, regulären Transaktionen, möglichst gering gehalten werden. Beides gewährleisten effektive Lösungen, welche jede einzelne Bestellung mittels ausgefeilter Analytik auf Betrugsverdacht überprüfen. Betrugsmuster wer-



den automatisiert erkannt und fließen direkt in Regelwerke ein, die eine fundierte Entscheidung gewährleisten. Integrierte Simulationsfunktionen, die auf der Basis von Bestandsdaten durchgeführt werden, sorgen dafür, dass die Regelsets kontinuierlich optimiert werden.

Besonders zielführend sind Tools, die auf die jeweilige Branche des Händlers abgestimmt sind. Denn je nach Branche kennzeichnen unterschiedliche Parameter eine verdächtige Transaktion. Ein Beispiel aus dem Handel: Bei riskanten Warengruppen wie Unterhaltungselektronik wird geprüft, ob das Land der kartenausgebenden Bank in plausibler Relation zum Land der Internetverbindung (IP-Adresse) steht. So würde eine französische Karte von einer russischen IP-Adresse abgelehnt, aber von IP-Adressen aus Monaco oder französischen Überseegebieten zugelassen werden.

Händler, die in das Risikomanagement auch ihre unternehmerische Zielsetzung einfließen lassen wollen, sollten auf eine Lösung setzen, welche die individuellen

Key Performance Indikatoren berücksichtigt. Moderne Systeme erlauben die Eingabe individueller Vorgaben. Wird beispielsweise eine maximale Betrugsrate definiert, ist das Raster engmaschiger,

d. h. eventuell werden Transaktionen abgelehnt, bei denen kein Betrug vorliegt. Der Shopanbieter nimmt also einen Umsatzverlust in Kauf. Steht umgekehrt ein Maximum an Umsatz im Vordergrund, werden die Maschen im Raster grober eingestellt. Dann wiederum muss der Händler mit mehr Zahlungsausfällen rechnen.

**Fazit**

Betrug nimmt vor allem im internationalen Online-Handel stetig an Raffinesse zu. Shopbetreiber sind also gut beraten, ein effektives Risikomanagementsystem zu installieren, das jede einzelne Transaktion in Echtzeit überprüft. In den letzten Jahren haben sich verschiedene Anbieter und Lösungen etabliert, die dafür sorgen, dass Schaden vom Händler abgewandt wird, bevor er ihn überhaupt trifft.

*Heiner Kallweit, Head of Product Line Risk & Fraud Prevention bei der Wirecard AG*

**Herr Kallweit, die Wirecard AG hat kürzlich ihr Portfolio im Risikomanagement um die Fraud Prevention Suite ergänzt. Was ist neu an der Lösung?**

Wir haben die Fraud Prevention Suite entwickelt, um unseren Kunden vor allem im internationalen Handel noch mehr Schutz zu bieten. Die Lösung erkennt Betrugsmuster noch schneller und zuverlässiger als derzeit verfügbare Lösungen – damit können Händler ihren Zahlungsausfall durch Betrug deutlich reduzieren.

**Wie hebt sich die Fraud Prevention Suite von vergleichbaren Angeboten des Wettbewerbs ab?**

Neben ihrer Geschwindigkeit, mit der die Fraud Prevention Suite mögliche Betrugsversuche aufdeckt, überzeugt deren branchenspezifische Ausrichtung. Wir haben die Lösung passgenau auf die Bedürfnisse der drei Kernbranchen des E-Commerce, Konsumgüter, Fluggesellschaften / Touristik und Digitale Güter, abgestimmt. Um die Ent-

scheidungsfindung zu optimieren, berücksichtigt die Fraud Prevention Suite jeweils genau die Faktoren, die im jeweiligen Bereich verdächtig sind. Parallel kann jeder Händler individuelle Key Performance Indikatoren bestimmen, die ebenfalls in das Regelwerk einfließen. Diese Kombination ist bislang einzigartig. Händler profitieren somit von standardisierten Einstellungen, die auf unserer jahrelangen Erfahrung beruhen und hat gleichzeitig die Möglichkeit, unternehmensspezifische Konfigurationen vorzunehmen.

**Für welche Kunden ist das Angebot interessant?**

Die Fraud Prevention Suite richtet sich ebenso an kleine Onlinehändler wie an große Unternehmen mit einem sehr hohen Transaktionsvolumen. Unabhängig davon, ob zehn oder tausend Kaufvorgänge in der Stunde eingehen – das System entscheidet in Sekundenbruchteilen über die Ablehnung oder Akzeptanz einer Zahlung.