Betrugsbekämpfung mit Unified Data

Von Attila Dogan,
Head of RevenueProtect

adyen

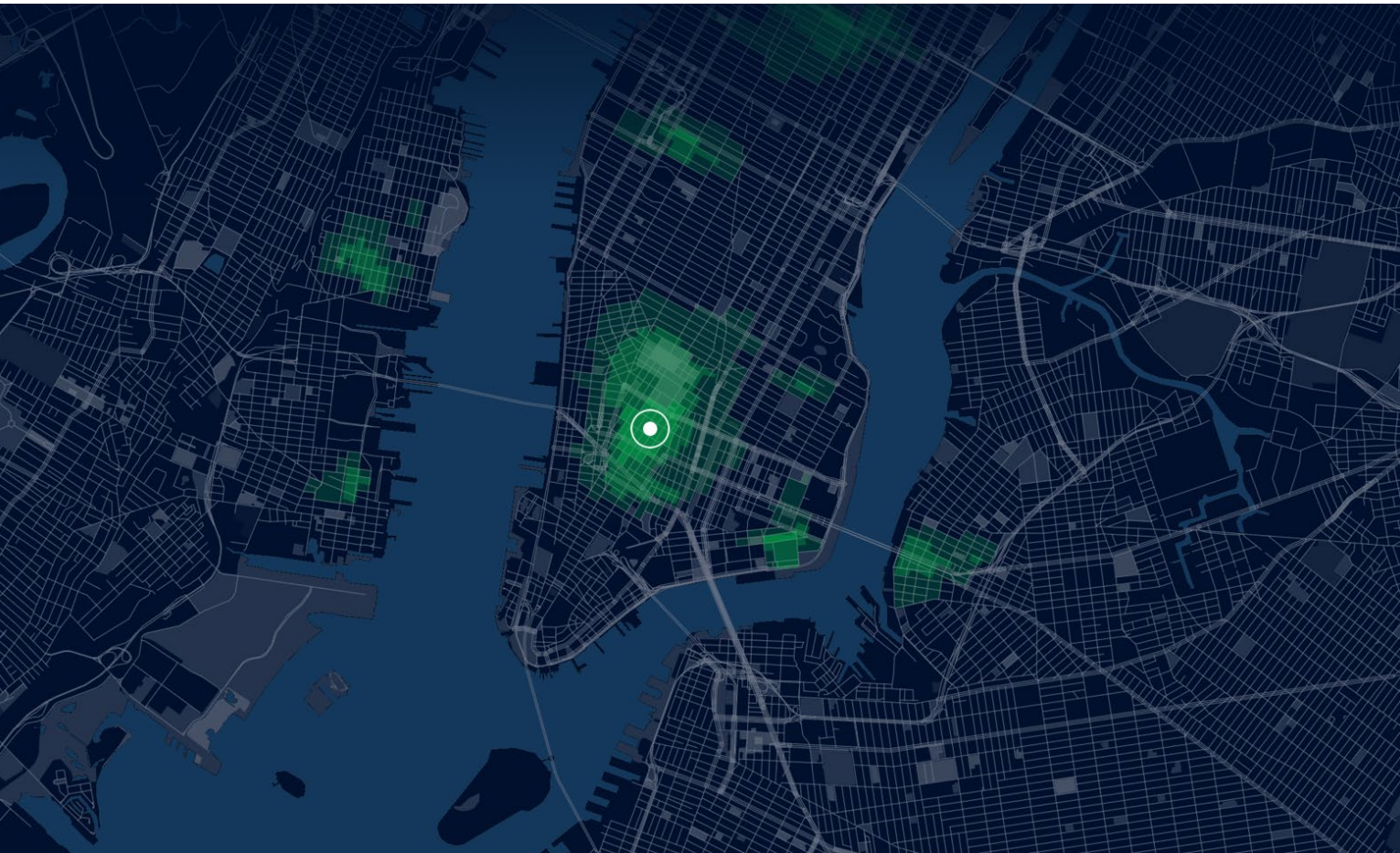
Unified Commerce ist nicht mehr wegzudenken

In Einzelhandelskreisen wurde schon viel über Unified Commerce geschrieben. Der Wechsel zu Unified Commerce, d.h. der Nutzung einer Technologieplattform zur Verbindung von allen Verkaufskanälen, also Käufen im Laden, auf mobilem Weg und über E-Commerce, wird so schnell nicht nachlassen. Forrester prognostiziert sogar, dass Cross-Channel-Einzelhandelsverkäufe in den USA in diesem Jahr 1,8 Milliarden US-Dollar erreichen werden.

Doch selbst während versierte Retail-Unternehmen ihre Modelle anpassen, um kanalübergreifend zu verkaufen, sind physische Ladenflächen alles andere als überholt.

Zum Überleben müssen Einzelhändler das Beste von beidem bieten – ein effizientes Ladenerlebnis und ein nahtloses digitales Erlebnis, das weder vom Standort, noch der Zahlungsmethode oder dem Gerät einzelner Käufer abhängt. Kauft jemand online und holt den Kauf im Laden ab? Kauft jemand im Laden und lässt die Ware nach Hause liefern? Kauft jemand über eine App und tauscht im Laden um? Die Möglichkeiten sind endlos.

Erfolgreiche Retailer müssen stets bemüht sein, ihren Kunden zahlreiche Optionen zum Einkauf und zur Zahlung zu bieten.



Betrugsbekämpfung mit nur einem Tool

Während viele Retailer einige offensichtliche Hürden im Unified Commerce wie zentralisiertes Bestellmanagement und die Transformation von Inventaren und Wertschöpfungsketten überwunden haben, bleibt die Frage: Was ist bei so vielen Transaktionsarten die beste Methode zur Betrugsbekämpfung?

Adyen entwickelt seit Jahren eine branchenführende Risikolösung für Unified Commerce. Jeder Kanal birgt eigene Risiken. Card Not Present (CNP), telefonische Bestellungen (MOTO) und Transaktionen im Laden (CP) verfügen allesamt über individuelle Eigenschaften und Risiken. Darum haben Retailer auf sie zugeschnittene Ansätze entwickelt, um mit den jeweiligen Herausforderungen umzugehen. Doch da die Risiken so unterschiedlich sind, ist eine einzige, einheitliche Plattform ideal, um sie alle zentral zu verwalten.

Aus vielen Gründen macht eine einheitliche Plattform nicht nur das Frontend einer Zahlungstransaktion effizienter – sie sorgt für Stabilität, Integrität und schließlich verbesserte Autorisierungsraten und Performance. Darüber hinaus eignet sich eine einheitliche Plattform auch zum besten Mittel zur Betrugsbekämpfung.

Durch eine Unified Plattform werden traditionell isolierte Informationen zusammengeführt. Zum Beispiel kann eine Zusammenführung der persönlichen Daten und der bisherigen Einkäufe von Kunden, die online und im Laden einkaufen, wichtige Erkenntnisse liefern.

Ein einziges Zahlungssystem muss Daten im gesamten Omnichannel-Netzwerk sofort identifizieren, einordnen und verbinden können. Der Balanceakt, ein nahtloses Einkaufserlebnis für Kunden zu schaffen, ohne das Gesamterlebnis zu trüben (das Betrugsmanagement muss für Kunden unsichtbar sein und darf keine zusätzlichen Hindernisse erzeugen), bildet das Kernstück unserer Vision von RevenueProtect von Adyen.

Alle verfügbaren Daten nutzen

Strategie- und Marketingabteilungen nutzen schon seit langem Daten, um das Verhalten und die Kaufgewohnheiten von Kunden zu verfolgen. Nun müssen diese Daten zunehmend auch im Sinne der Bekämpfung von Zahlungsbetrügern genutzt werden.

Nehmen wir zum Beispiel einen Händler in New York City. Er könnte mit anonymisierten Daten (IP-Standorte und Rechnungsadressen) Heatmaps von Kunden erstellen lassen, die online einkaufen und ihre Ware in einem Geschäft abholen möchten. Die Muster geben dem Händler sowohl einen Überblick über die Kaufgewohnheiten seiner Kunden als auch Messwerte, um Betrugsversuche aufzudecken. Transaktionen, die vom Muster abweichen, erregen sofort Verdacht.

Wer kauft wo (und wie)?

Entscheidet sich der Händler zu expandieren, können Daten anonymisiert genutzt werden, um aktive Kundengruppen zu erkennen, die zwar online einkaufen, aber aufgrund der Entfernung keines der Geschäfte persönlich aufsuchen können (siehe die gelb markierte Nachbarschaft). Die gelbe Nachbarschaft zeigt demnach, wo die Nachfrage nach Produkten eines Händlers bereits messbar hoch ist.

Wichtige Erkenntnisse durch Dateneinblick

Stellen Sie sich vor, ein Kunde betritt einen Laden im Stadtteil Soho in London. Er kauft beispielsweise ein Paar Schuhe über ein Point-of-Sale-Terminal, bestätigt mit PIN (ein ideales Szenario für jeden Betrugsmanager, da sich die Haftungspflicht zugunsten des Retailers umkehrt).
Am selben Abend kauft derselbe Kunde ein zusätzliches Paar Socken auf der Website des Einzelhändlers. Seine IP-Adresse wird keine 20 Kilometer vom Laden entfernt registriert, den er vor ein paar Stunden besucht hat.

Selbst wenn der Kunde bei seinem Online-Einkauf eine andere Kreditkarte verwendet (was aufgrund der noch nicht vorhandenen bisherigen Käuferdaten als größeres Risiko eingestuft werden könnte), wüsste der Retailer, dass er diesen neuen Einkauf zulassen könnte. Millionen von korrelierten Datensätzen sagen ihm nämlich, dass die Wahrscheinlichkeit, dass es sich hier um eine echte Bestellung handelt, außergewöhnlich hoch ist.

In einem ähnlichen Szenario besucht ein Kunde, der bereits zahlreiche Online-Käufe getätigt hat, eines Tages ein Geschäft. Ausgerechnet an diesem Tag versagt die Chip-und-PIN-Kombination des Käufers. Doch wenn das Betrugsmanagementsystem die zahlreichen bisherigen Online-Käufe des Käufers zusammen mit einer Anschrift in der Nähe erkennt, akzeptiert es eher ein einfaches Durchziehen der Karte (Magnetstreifen-Fallback), auch wenn es dies von einer völlig unbekannten Person ablehnen würde.

Daten können auch die Alarmglocken läuten lassen

Eine gute Zahlungsplattform kann zwar Licht auf subtile Kundeninteraktionen werfen, aber sie sollte auch weniger auffällige bemerken. Wenn Karten zum Beispiel an einem Standort verwendet werden und Minuten später hunderte Kilometer weiter auftauchen, ist das sofort ein Warnsignal für betrügerische Käufe.

Mit Bedacht blockieren

Seit Jahrzehnten entwickeln Retailer (und eigentlich alle Organisationen, die Zahlungen annehmen) manuelle, kanalspezifische Lösungen zur Betrugsabwehr.
Sowohl Chip als auch PIN zu verlangen, ist ein reiner Authentifizierungsmechanismus für den Laden, so wie 3-D Secure Online-Transaktionen absichert. Als die Tools noch einfacher waren und E-Commerce noch neu war, reichten manuelle Prüfungen und individuelle Betrachtungen einzelner Fälle völlig aus.

Doch E-Commerce ist inzwischen ein globaler Wirtschaftszweig und Geschwindigkeit beim Checkout ist sowohl im physischen als auch im digitalen Bereich unerlässlich. In dieser neuen Welt des gemischten Handels ist es heutzutage so wichtig wie nie zuvor, ein Zahlungssystem zu haben, das Daten aus allen Kanälen nutzt, um Händlern dabei zu helfen, smarte Entscheidungen zu treffen.

Abraham Maslow schrieb: „Wenn man als Werkzeug nur einen Hammer hat, sieht jedes Problem wie ein Nagel aus.“ Doch für E-Commerce und im Einzelhandel ist der Hammer häufig ein zu stumpfes Werkzeug. Beim Betrugsmanagement geht es nicht nur darum, „schlechte“ Transaktionen zu vermeiden, sondern auch darum, die „guten“ möglichst reibungslos zu verarbeiten. Ein ganzheitlicher Betrugsmanagementansatz, bei dem alle verfügbaren Daten in einem System zusammengeführt werden, ist nicht nur der effektivste Ansatz zur Betrugsbekämpfung, sondern steigert langfristig auch den Umsatz, indem er Unternehmen ein durchdachtes Toolkit für ein kompliziertes Problem an die Hand gibt.

Über Adyen

Adyen ist die bevorzugte Zahlungsplattform für weltweit führende Unternehmen. Als einziger Anbieter einer modernen End-to-End-Infrastruktur, die Händler direkt mit Visa, MasterCard sowie weltweit von Verbrauchern bevorzugten Zahlungsmethoden verbindet, bietet Adyen reibungslose Zahlungsabläufe – online, auf Mobilgeräten und am Point-of-Sale. Adyen hat Niederlassungen rund um den Globus und zählt bereits mehr als 4.500 Unternehmen zu seinen Kunden, darunter acht der zehn größten US-amerikanischen Internet-Firmen. Zu unseren Kunden gehören Facebook, Delivery Hero, Netflix, Spotify, L'Oreal und Burberry.

Über den Autor

Attila Dogan ist Head of RevenueProtect bei dyen und betreut die Produktentwicklung der Betrugsmanagementlösung. Bevor Attila dem Unternehmen beitrat, verbrachte er für zahlreiche E-Commerce-Unternehmen selbst 16 Jahre auf der Händlerseite und war Beiratsmitglied im Merchant Risk Council.