global CT | WHITEPAPER

FRAUD MANAGEMENT

im E-Commerce

Die global CT ist eine inhabergeführte Unternehmensgruppe mit Hauptsitz in Hannover-Isernhagen. Mit unseren Geschäftsbereichen global CT Consulting & global CT Digital begleiten wir Unternehmen auf ihrem digitalen Transformationsweg. Hierbei verfolgen wir einen ganzheitlichen, menschenzentrierten Beratungsansatz, um in partnerschaftlicher Zusammenarbeit mit unseren Kunden individuelle Lösungen zu entwickeln. Dabei setzen wir auf zeitgemäße Arbeitsweisen & Methoden von der Beratung bis zur Softwareentwicklung.

global CT Services & Consulting GmbH • Lorbeerrosenweg 8 • 30916 Isernhagen • P +49 511 515 107 10 • F +49 511 515 107 35 • info@globalct.com • www.globalct.com • Geschäftsführer: Naser Capric, Florian Toussaint, Philip Lutz • HRB 212883 • Ust-Idnr. DE301609314

Fraud Management Whitepaper

Herausgegeben von der global CT Services & Consulting GmbH

Von Liu, Lu

global CT Services & Consulting GmbH • Lorbeerrosenweg 8 • 30916 Isernhagen • P +49 511 515 107 10 • F +49 511 515 107 35 • info@globalct.com • www.globalct.com • Geschäftsführer: Naser Capric, Florian Toussaint, Philip Lutz • HRB 212883 • Ust-Idnr. DE301609314

VORWORT

Jedes Unternehmen kann von Fraud betroffen sein: Ob mittelständischer Betrieb, Konzern oder öffentliche Institutionen. Daraus ergeben sich jährlich Schäden in Milliardenhöhe. Dazu zählen jedoch nicht nur finanzielle Einbußen, sondern auch der massive Vertrauensverlust, den der Betrug in Firmen und Organisationen anrichtet. Um dieses Problem möglichst im Keim zu ersticken, sollten Unternehmen proaktiv handeln. Wer vorausschauend handelt, kann Betrug eingrenzen die Kundenbindung stärken, Gewinne sichern und Kosten vermeiden.

Es ist aber weder wirtschaftlich noch realistisch, sämtliche Betrugsrisiken zu eliminieren. Das Ziel sollte sein, die Gefahren und somit die Anzahl der Fälle auf ein Minimum zu reduzieren. Dabei ist es wichtig, möglichst kostendeckend zu arbeiten, damit der betriebene Aufwand nicht die Verluste übersteigt. Unternehmen stehen dabei vor verschiedenen Herausforderungen wie zum Beispiel aufkommende Betrugstrends, die sich ständig verändern, organisierte kriminelle Netzwerke, unterschiedliche Datenquellen und Datenqualitäten. Aber die zentrale Herausforderung für E-Commerce Händler ist immer der Balanceakt: Wie kann ich mein Geschäft ausbauen und dabei die Kosten für Betrug in den Griff bekommen, während ich gleichzeitig das Vertrauen und die Loyalität meiner Kunden stärke?

Gemeinsam mit unseren Kunden meistern wir diese Herausforderungen und rüsten sie mit dem notwendigen Handwerkszeug aus. Die global CT setzt dabei auf ein systematisches Vorgehen. Mit unserem Know-how begleiten wir unsere Kunden von Anfang an professionell, um am Ende des Vorhabens eine sichere und optimale Lösung zu erreichen.

Die von uns betreuten Unternehmen und Organisationen können mit Hilfe unserer Analyse schnell wichtige Zusammenhänge und Abhängigkeiten verstehen, um anschließend dem E-Commerce-Betrug bestmöglich vorzubeugen und somit einzugrenzen. Mit unserem Ansatz besteht nicht nur die Möglichkeit, vorhandene Betrugsfälle zu erkennen, sondern auch mit einem maßgeschneiderten Modell Voraussagen zu treffen. Mit diesem werden verdächtige Fälle bereits im Vorfeld erkannt, bevor der Schaden eintritt.

INHALTSVERZEICHNIS

Abkürzungsverzeichnis

Abkürzung	Bedeutung
BA.	Bundesagentur für Arbeit.
BRMS	Business-Rule-Management-Systems
RPA	Robotic Prozess Automation
QA	Quality Assurance
KPI	Key Performance Indicator (Leistungskennzahlen)
CAGR	Compound Annual Growth Rate
FMS	Fraud Management System

Abbildungsverzeichnis

1.EINLEITUNG

1.1.Einleitung in die Thematik

Weltweit verlieren Unternehmen etwa fünf Prozent ihrer jährlichen Einnahmen durch Betrug, was global zu potenziellen Verlusten von mehr als 5 Billionen Euro führt.[1] Dazu zählen nicht nur finanzielle Einbußen, sondern auch der entstandene massive Vertrauensverlust, den dieses Szenario zur Folge hat. Dies trifft besonders auf öffentliche Institutionen wie Behörden und Ämter zu. Während die Summe des unmittelbaren Betrugsverlustes durchaus schwankt, so sind die tatsächlichen Kosten in den Bereichen Produktivitätsverlust und Verlust des Kundenvertrauens viel höher einzuordnen. Ebenso immens ist der Betrag, den der Schaden durch unentdeckten Betrug verursacht.

Nicht nur Unternehmen aus der freien Wirtschaft sind von Betrug betroffen, sondern auch der öffentliche Sektor, wie das folgende Beispiel erläutert. Unter anderem hat es bei der Bundesagentur für Arbeit Betrugsfälle bei der Beantragung von Corona-Soforthilfen gegeben. Ein Unternehmer strich mit gefälschten Anträgen rund 7,4 Millionen Euro ein. Dieser soll 90 Mitarbeiter für seine Beratungsfirma erfunden und mit Hilfe von illegal erworbenen Sozialversicherungsdaten Kurzarbeitergeld erhalten haben, ehe er von der Polizei festgenommen wurde.[2]

Einige Zahlen in diesem Zusammenhang: Die Bundesagentur für Arbeit zahlte eine Milliarde Euro Kurzarbeitergeld pro Woche an Unternehmen aus (Stand Juli 2020). Allein im April vergangenen Jahres hat diese fast 6,9 Millionen Beschäftigte in 565.000 Unternehmen mit Kurzarbeitergeld vergütet - das betrifft somit jeden fünften Arbeitnehmer in Deutschland. Zum Vergleich: In der Finanzkrise 2008/09 wurden zu Hochzeiten (Juli 2009) 61.400 Betrieben Kurzarbeitergeld genehmigt. Die heutigen Zahlen entsprechen damit in etwa der zehnfachen Summe von damals.[3]

Mit der steigenden Anzahl von Anträgen wächst für Betrüger auch die Chance, erfolgreich Missbrauch zu begehen. Die Staatsanwaltschaften rechneten zum Ende des Jahres 2020 mit einem deutlich erhöhten Aufkommen an Ermittlungsverfahren gegen mutmaßlich betrügerische Unternehmen. Im Fall der Corona-Soforthilfen für Kleinunternehmen geht die Zahl der staatsanwaltschaftlichen Ermittlungsverfahren bereits in die Tausende. Allein die Staatsanwaltschaft Berlin führt derzeit mehr als 870 Verfahren mit einer Schadenssumme von über sechs Millionen Euro. Die Zahl wird sich aller Voraussicht nach in der nächsten Zeit deutlich erhöhen.[4]

Das Resultat daraus ist, dass Behörden konsequenter als bisher gegen Betrug vorgehen müssen. Dabei gilt es, eine Vielzahl von Herausforderungen zu meistern, um Betrug rechtzeitig zu erkennen und zu verhindern.

[1] Vgl. Crow Global (2019).
[2] Vgl. Halbach. A. (2020).
[3] Vgl. Groeneveld. J, (2020).
[4] Vgl. Halbach. A. (2020).

Im Vergleich zu anderen Anbietern auf dem Markt, die sich auf Betrugsprävention innerhalb einer Organisation oder eines Unternehmens spezialisiert haben - dazu zählen unter anderem Anti-Korruption, Geldwäscheprävention, Compliance, Forensik und interne Revision, konzentriert sich die global CT speziell auf externen Betrug im Bereich der Online-Zahlung im E-Commerce, auch als Order-to-Cash-Prozess bekannt. Darunter ist der gesamte Ablauf vom Eingang einer Kundenbestellung bis hin zur Bezahlung der offenen Forderung durch den Kunden zu verstehen. Im öffentlichen Sektor liegt unser Fokus auf Betrugsprävention im Bereich Sozialleistungen.

E-Commerce boomt

Der Trend ist klar, Online-Shopping mit den Vorteilen von der großen Auswahl, dem einfachen Preis- und Produktvergleich, dem stressfreien Einkauf unabhängig von Öffnungszeiten oder Verkehrslage und der bequemen Lieferung wird immer beliebter. Die E-Commerce-Branche verzeichnet durch die Corona-Pandemie einen deutlichen Aufschwung. Immer mehr Menschen entscheiden sich dafür, Waren und Dienstleistungen online einzukaufen. Für das Jahr 2025 wird ein Marktvolumen von 3.079.028 Mio. € prognostiziert. Dies entspricht einem erwarteten jährlichen Umsatzwachstum von 6,29 Pozent (CAGR 2021-2025).[5] Im Jahr 2018 wurde jeder zehnte Euro, der weltweit gezahlt worden ist, online ausgegeben. Voraussagen nach werden ab 2022 17 Prozent des weltweiten Handels online abgewickelt.[6]

Covid-19 Auswirkung auf das E-Commerce Geschäft mehr postiv als negativ

Im April 2020 war etwa ein Drittel der Weltbevölkerung in irgendeiner Form vom Lockdown betroffen. Dies wiederum führte weltweit zu einem Anstieg der E-Commerce-Transaktionen. In Großbritannien stieg beispielsweise das Bestellvolumen im Online-Handel bei einigen Produkten um mehr als 200 Prozent.[7] Der Anstieg der E-Commerce-Transaktionen erreichte seinen Höchststand in der Zeit der strengsten Einschränkungen. Es gibt auch insgesamt immer noch einen signifikanten Anstieg der Online-Einkaufsaktivitäten im Vergleich zum Niveau vor der Pandemie zu beobachten.

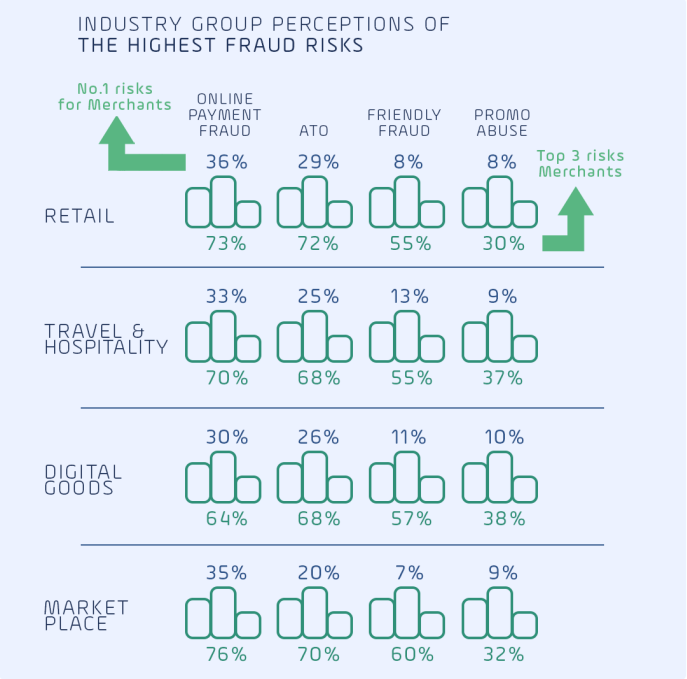
Ebenso wurden Lieferdienste aufgrund sozialer Abgrenzungsmaßnahmen stark nachgefragt. Ein Anstieg der Essenslieferungen wurde aufgrund der Corona-Maßnahmen ausgelöst. Da Restaurantbesuche untersagt waren, boten viele Restaurants eine Abholoption an. Dieser enorme Anstieg der Online-Transaktionen könnte eine Erklärung dafür sein, warum zum Zeitpunkt dieser Umfrage eine Mehrheit der Händler die Auswirkungen von Covid-19 eher positiv als negativ bewertet haben. 46 Prozent aller Teilnehmer gaben außerdem an, dass die Folgen der weltweiten Covid-19-Pandemie auf ihre Geschäfte positiv oder als sehr positiv zu beurteilen sind. Positiv könnte in diesem Fall bedeuten, dass sie mehr Volumen verzeichnen.[8]

Daten und Fakten zum E-Commerce-Betrug

Im Jahr 2020 waren 74 Prozent der Organisationen und Unternehmen von Online-Zahlungsbetrug betroffen.[9] Fast drei Viertel der Unternehmen geben an, dass dieser Fakt ein großes Problem darstellt.[10] Voraussichtlich werden den Online-Händlern somit zwischen 2018 und 2023 insgesamt 130 Milliarden Euro an Umsatz entgehen.[11]

Online-Betrug kostet E-Commerce Unternehmen rund 1,88 Prozent ihrer Einnahmen.[12] Ein Beispiel: Für jeden Ein-Euro-Betrug verlieren E-Commerce-Unternehmen durch Rückbuchungen zusätzlich 2,1 Euro.[13] Die Betrugskosten setzen sich für Firmen und Organisationen unter anderem aus Rückbuchungsgebühren,

[5] Vgl. o. V.: Statista Marktprognose.
[6] Vgl. o. V.: Statista statistics.
[7] Vgl. o. V. (2020): Online Merchant Perspectives, S. 8.
[8] Vgl. ebd. S8.
[9] Vgl. JP Morgen (2021).
[10] Vgl. Experian plc (2018).
[11] Vgl. Morrow, S.; Maynard, M (2020).
[12] Vgl. LexisNexis Risk Solutions (2018), S. 14.
[13] Vgl. LexisNexis Risk Solutions (2020), S. 9.



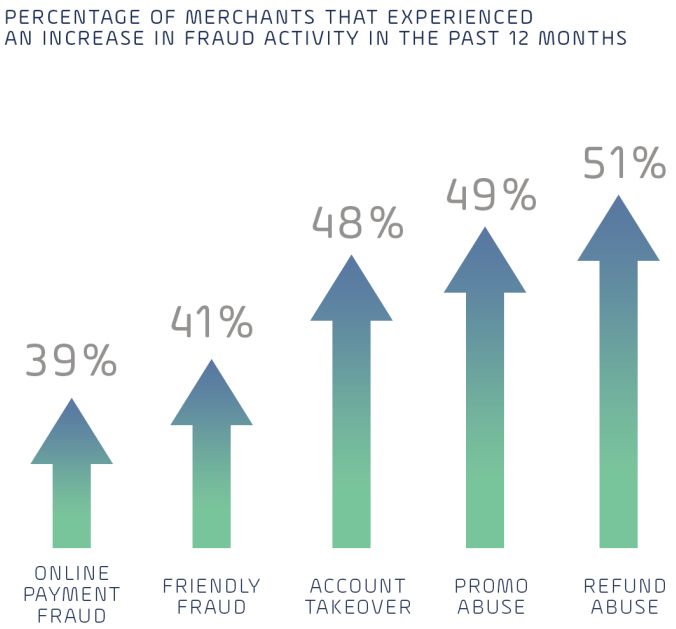


Abbildung 1 – Top-Bedrohungen im E-Commerce Fraud[14]

Transportkosten sowie Kosten für Betrugsermittlung, Strafverfolgung und IT-Security zusammen.

Es geht bei diesem Thema aber nicht nur um die finanziellen Kosten, sondern auch um die Auswirkungen des Betrugs auf die Marken- und Kundentreue. Die Verbraucherinnen und Verbraucher fallen dem Betrug z. B. durch Identitätsdiebstahl zum Opfer. Oftmals sind sie sich aus Unwissenheit nicht bewusst, wie diese Art von Betrug funktioniert. Daher machen sie häufig die Online-Händler hierfür verantwortlich. Eine mögliche Konsequenz ist, dass die Betroffenen aufgrund des Vertrauensverlustes zukünftig nicht mehr auf den betroffenen Websites einkaufen.

Bei einem Online-Betrug geht es nicht nur um den materiellen Verlust: Ist ein Angriff erfolgreich, wird er mit großer Wahrscheinlichkeit wiederholt.

Betrugsprävention schützt in diesem Fall die Prozesse und somit Unternehmen vor gefälschten Identitäten, Identitätsübernahmen, fremden Kontoübernahmen, friendly fraud (Rückbuchungsbetrug) und allen anderen Betrugsmustern, denen wir über die Jahre begegnet sind.

Mit Online-Zahlungen steigt auch die Zahl der Betrugsfälle

Die Betrugsversuche im E-Commerce-Bereich nehmen deutlich zu und werden zudem immer ausgefeilter und undurchsichtiger. Bereits 90 Prozent der Händler sind mit Betrug in Berührung ausgefeilter und undurchsichtiger. Dabei werden durchschnittlich insgesamt drei Prozent der Bestellungen im Online-Shop vom Händler als Betrug klassifiziert.

[14] Quelle: o. V. (2020): Online Merchant Perspectives, S. 28 f.

Der Umsatzverlust durch Betrug liegt im Durchschnitt bei zwei Prozent.[14]

Das bedeutet, E-Commerce Unternehmen in Deutschland verlieren rund 1,68 Milliarden Euro im Jahr 2021 (bezogen auf den Gesamtumsatz des deutschen E-Commerce-Gesamtumsatzes von 84,123 Milliarden. Euro brutto).[15]

Betrug im Online-Zahlungsverkehr ist die größte Bedrohung für E-Commerce Unternehmen. In diesem Bereich nehmen Account Takeover (Kontoübernahmen) sowie Promotion- und Retoure-Missbrauch deutlich zu. Diese Betrugsart ist immer noch die Nummer eins unter den Betrugsdelikten, wobei die Kontoübernahmen knapp vor dem friendly fraud (Rückbuchungsbetrug) an zweiter Stelle liegt. Fast 50 Prozent der Händler haben berichtet, dass Retour- und Promotionsmissbrauch deutlich zugenommen haben, was mit dem veränderten Kaufverhalten aufgrund von Covid-19 zusammenhängt. Datenschutzverletzungen und damit verbundene Geldstrafen sind die größten Sorgen der Händler in Bezug auf Kontoübernahmen.

Es besteht Grund zur Annahme, dass der signifikante Anstieg des Retourenmissbrauchs (Refund) im Einzelhandel und auf Marktplätzen mit der Zunahme der kontaktlosen Warenlieferung zusammenhängen könnte. Während der Covid-19-Pandemie kündigten viele Online-Händler an, dass Zusteller die Produkte künftig vor der Haustür der Kunden abstellen, anstatt diese persönlich zu übergeben. Das könnte zur Folge haben, dass die Lieferung möglicherweise nicht vom Kunden bestätigt wird und dieser folglich die Möglichkeit hat, zu behaupten, er habe die Ware nie erhalten.

[15] Vgl. Meier, J. (2020).
[16] Vgl. Statista (2021).

1.2. Herausforderung

Obwohl die meisten Banken, viele Online-Händler sowie einige öffentliche Einrichtungen über Betrugserkennungssysteme verfügen, bieten diese in der Regel nur eine reaktive und somit nachträgliche Prüfung und Analyse auffälliger Transaktionen. Dieser oftmals zu späte Ansatz bietet keinen wirklichen Schutz vor Verlust. Eine Echtzeitbewertung ist in diesem Fall die beste Option, um Betrug zu verhindern.

Die Zunahme der Komplexität in den einzelnen Geschäftsbereichen, technische Infrastrukturen, bereichsübergreifende Arbeitsprozesse und Umbrüche in der Organisationsstruktur von Instituten führen oftmals dazu, dass sich die Wahrscheinlichkeit des Nichtentdeckens von wirtschaftskriminellen Handlungen weiter erhöht.[17]

Wir stehen hierbei vor verschiedenen Herausforderungen: [18]

- Auf aufkommende Betrugstrends, die sich zudem ständig verändern, muss besonders schnell reagiert werden, um die Betrugswelle rechtzeitig zu stoppen.

- In organisierten, kriminellen Netzwerken sind immer mehr trickreiche Betrüger aktiv. Darauf gilt es sich einzustellen und zu handeln.

- Die derzeit eingesetzten Systeme bringen technologische Einschränkungen mit sich, die nur unzureichend analytische Modellierung unterstützen und zudem die Bestimmung der Echtheit der Transaktion verlangsamen können. (Anmerkung: Analytische Modelle stützen sich auf Algorithmen, erkennen Muster in Datenmengen und verwandeln sie in mathematische Gleichungen).

- Von mehreren Standorten agierende Unternehmen haben mit der Schwierigkeit zu kämpfen, dass unterschiedliche Datenquellen und Datenqualitäten den Zugriff auf die richtigen Informationen im richtigen Format aus unterschiedlichen Vorsystemen erschweren. Statistische Systeme und Systeme, die aus Beispielen lernen und diese nach Beendigung der Lernphase verallgemeinern, benötigen einheitliche und fehlerbereinigte Daten aus den beteiligten Systemen, um brauchbare Ergebnisse zu erzielen.

- Knappe Ressourcen und eine geringe Anzahl von Fachleuten auf dem Markt sind qualitative und quantitative Hindernisse, um die notwendigen Anforderungen zu erkennen und Maßnahmen umzusetzen.

- Die Weiterentwicklung der Compliance-Anforderungen ist ein ständiger Kampf, um mit den sich stetig ändernden Rahmenbedingungen Schritt zu halten.[19]

- Die Sammlung von persönlichen Daten und die damit verbundenen Datenschutzbedenken sind von den gesetzlichen Regeln abhängig. Folgende Fragen kommen dabei auf: Welche Daten dürfen wir sammeln und verarbeiten und welche sind für eine sinnvolle Analyse verfügbar?

- Ethische Fragestellungen zu diesem Thema: Wann werden bestimmte Personengruppen diskriminiert? Sind von Maschinen getroffene Entscheidungen über menschliche Schicksale vertretbar? Denn die Frage der Nutzung großer Datenbestände mit dem Ziel, Muster und Zusammenhänge zu erkennen, um richtige Entscheidungen zu treffen oder darüber hinaus Prognosen zu liefern, ist bei weitem keine rein technologische Herausforderung. Der Kern der Frage ist: Kann ein Algorithmus irren? Hier wird deutlich, dass noch viele ethische und auch rechtliche Fragestellungen geklärt werden müssen.[20]

[17] Vgl. Nehls, N.; Otto, Michael (2015), S. 6.
[18] Vgl. o. V. (2015): SAS Fraud Management.
[19] Vgl. o. V. (2015): SAS Fraud Management.
[20] Vgl. Buchmann.T (2019) S. 20.

Die zentrale Herausforderung für E-Commerce Händler ist immer der Balanceakt: Wie kann ich mein Geschäft ausbauen und dabei die Kosten für Betrug in den Griff bekommen, während ich gleichzeitig das Vertrauen und die Loyalität meiner Kunden stärke?

1.3. Definition Fraud und Fraud-Management

Fraud ist der englische Begriff für Betrug und bedeutet eine bewusste Handlung, mit der andere getäuscht werden, um in den meisten Fällen einen finanziellen Gewinn daraus zu erzielen.[21]

Definition von Fraud-Management

Der Umgang von betrügerischen Handlungen und andere unternehmensschädlichen Aktivitäten wie zum Beispiel Bilanzmanipulationen, Unterschlagung oder Untreue nach wirtschaftlichen Gesichtspunkten wird als Fraud-Management bezeichnet. Dieses beinhaltet sämtliche Maßnahmen wie Prävention, Erkennung, Analyse und Aufarbeitung von Fraud-Fällen. Schadensbeseitigung und Optimierung des Systems, sprich Regelwerke, sind ebenso ein wichtiger Bestandteil.

Kategorien

Im Fraud-Management werden alle organisationsrelevanten (externe und interne) Betrugskategorien gemanagt. Extern bezeichnet einen Angriff von außen und besteht hauptsächlich aus:[22]

- falschen Identitäten sowie manipulierten Informationen,
- extern verursachte Vermögensdelikte, auch Diebstahl intellektuellen Kapitals,
- Korruption.

Im Gegensatz dazu wird interner Betrug - beispielsweise Missbrauch von Eigentum innerhalb einer Organisation - häufig auch als berufsbedingter Betrug bezeichnet. Dazu gehören:

- Finanzmanipulationen, auch Bilanzbetrug genannt,
- unternehmensintern verursachte Vermögensschädigungen,
- Korruption.

Wie funktioniert Fraud-Management?

Bevor wir zur Erläuterung kommen, wie Fraud-Management funktioniert, ist es wichtig, vorab zu verstehen, dass jede Organisation und jedes Unternehmen Betrug zum Opfer fallen kann. Es ist allerdings weder realistisch noch ökonomisch, Betrugsfälle komplett zu eliminieren. Das Ziel ist, ein akzeptables Risikomaß zu erreichen und dabei kosteneffizient zu arbeiten. Dies ist eine zwingende Voraussetzung, damit die Investitionen in Technologie, Prozesse und Personal sowie in Hilfsmitteln die kalkulierten Betrugskosten nicht übersteigen. Erst wenn Verständnis darüber erlangt wurde, wie Betrug zu Stande kommt, kann ein effizientes Fraud Management System im Unternehmen installiert werden.[23]

Fraud-Management erstreckt sich über drei Prozesse:[24]

- Prävention
- Aufdeckung und
- Aufarbeitung

Prävention

Um eine wirksame Prävention zu forcieren, muss den Unternehmen oder Organisationen bewusst sein, warum es zu Betrugsdelikten kommt und wie diese ablaufen. Eigene Daten oder Daten aus anderen Unternehmen, die aus bestätigten Betrugsfällen resultieren, können diesbezügliche Fragen am besten beantworten. Das Sammeln und Analysieren von historischen Daten spielen dabei eine wichtige Rolle.

Aufdeckung

Sobald ein Kunde oder eine Transaktion Auffälligkeiten aufweisen, greift der Aufdeckungsprozess. Dabei spielen neue Technologien eine wichtige Rolle. Das Vorgehen besteht aus Techniken und manuellen

[21] Vgl. Siller, H. (2018).
[22] Vgl. Schuchter, A. (2017).
[23] Vgl. ebd.
[24] Vgl. Schuchter, A. (2017).

Prozessschritten, um Klarheit zu schaffen und den Verdacht bis hin zum konkreten Betrugsfall zu identifizieren.

Aufarbeitung

Der dritte Hauptprozess im Fraud-Management arbeitet erkannte Fälle von Wirtschaftskriminalität auf - allerdings nicht im strafrechtlichen Sinn. Fraud-Manager konzentrieren sich auf forensische Prüfungen, um aus aufgedeckten Fällen auf weitere kriminelle Strukturen zu schließen oder Verluste bei den Verantwortlichen zurückholen zu können. Auch die Optimierung von Techniken und manuellen Prüfprozessen zählen zur Aufarbeitung im Fraud-Management. Dabei spielt der Kalibrierungsprozess eine wichtige Rolle. Dieser beinhaltet eine Messung von bekannter Größe oder Richtigkeit (z. B. historische Daten) und besteht aus den Ergebnissen der manuellen Prüfung, die im Rahmen einer Rückkopplungsschleife (Feedback-Loop) im Kalibrierungsprozess und damit auch in den Regelwerken Berücksichtigung finden.

2.BETRUGSPRÄVENTION

2.1.Unser Verständnis eines effektiven Fraud Management Systems

Nach unserem Verständnis sollte ein effektives Fraud Management System auf dem Zusammenspiel zwischen MI (Menschlicher Intelligenz) und KI (Künstlicher Intelligenz) basieren, ergänzt durch einen Predictive Analytics Ansatz. Predictive Analytics ist die Verwendung von Daten, statistischen Algorithmen und Machine-Learning Techniken, um die Wahrscheinlichkeit zukünftiger Ergebnisse auf der Grundlage historischer Daten zu ermitteln. Das Ziel ist es, über das Wissen, was geschehen ist, hinauszugehen und eine bestmögliche Einschätzung dessen zu geben, was in der Zukunft geschehen wird.[25]

Die Kombination mehrerer Analysemethoden kann die Betrugsmustererkennung verbessern und kriminelles Verhalten verhindern. Da das Thema Betrug im E-Commerce immer mehr an Bedeutung gewinnt, untersucht eine leistungsstarke Verhaltensanalyse alle Aktionen in einem Netzwerk in Echtzeit, um Anomalien zu erkennen, die auf Betrug hinweisen können.[26]

„Wir sehen einen klaren Trend hin zur Unterstützung durch automatisierte Systeme. Viele Betrugsversuche können heute schon automatisiert erkannt und verhindert werden. Gleichzeitig müssen wir in der Lage sein, auf die Dynamiken in den Angriffsvektoren reagieren zu können. Daher setzen wir weiterhin auf hochspezialisierte, operative Teams, um neue oder bislang unentdeckte Betrugsmuster zu erforschen."

Simon Eder, Zalando[27]

[25] o. V. (o. J.) Predictive Analytics.

[26] o. V. (o. J.) Predictive Analytics.
[27] Vgl. Meier, J. (2020).

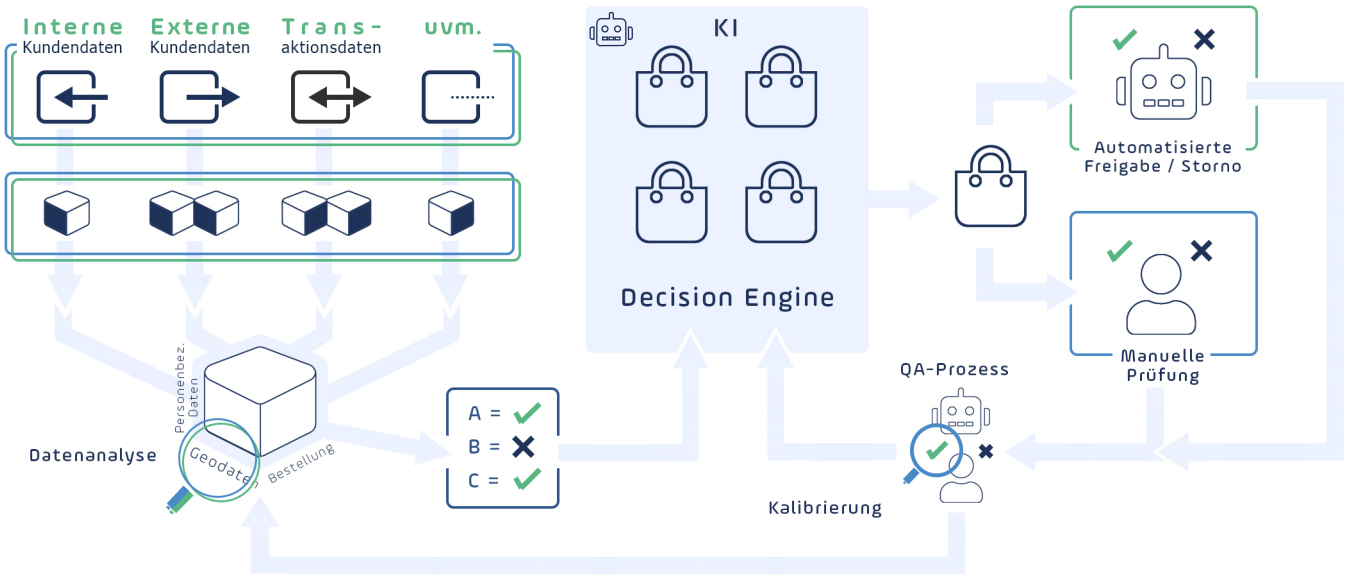


Abbildung 2 – Übersicht eines ganzheitlichen Fraud Managements[28]

Schritt 1

Identifikation der zur Betrugsprävention relevanten Datenquellen (z. B. interne & externe Kundendaten, Transaktionsdaten etc.). Aggregation und Extrahierung der erforderlichen Daten aus den identifizierten Quellen. Die gesammelten Daten werden zu einem Datenmodell integriert und in einen Zustand formatiert, der für die Erstellung von Geschäftsregeln und statistischen Modellen geeignet ist, um potenziell betrügerische Transaktionen zu identifizieren.

Schritt 2

Auswahl und Einsatz datenanalytischer Methoden (z. B. Decision Tree, Logistic Regression, Text Mining etc.) zwecks Identifizierung und Validierung von Transaktionszusammenhänge. Ergebnisse der Datenanalyse werden von Fraud-Experten validiert und abgenommen. State-of-the-Art Machine Learning sorgt für höchste Trennschärfe. Parallel werden die Erfahrungen und das Wissen der Fraud-Expertenvalidiert und abgenommen. State-of-the-Art
Machine Learning sorgt für höchste Trennschärfe.
Parallel werden die Erfahrungen und das Wissen der Fraud-Experten zusammengetragen und konsolidiert. Die langjährige Fraud Expertise sorgt für hohe Transparenz und Erklärbarkeit.

Schritt 3

Die Ergebnisse aus der Datenanalyse sowie die Erfahrungen und das Wissen der Fraud-Experten werden zur Erstellung des Regelwerks (Prüfregeln) herangezogen und dienen als Input für die Decision Engine.

Schritt 4

Die Decision-Engine identifiziert anhand des Regelwerks auffällige Transaktionen und steuert diese entweder zur manuellen Prüfung aus, oder es erfolgt eine automatisierte Freigabe bzw. ein automatisiertes Storno.

[28] Quelle: Eigene Darstellung.

Schritt 5

Die Fraud-Analysten prüfen den Sachverhalt und treffen eine Entscheidung (Betrug oder falscher Alarm). Im Rahmen eines QA-Prozesses können stichprobenhaft die Entscheidungen der Fraud-Analysten geprüft werden.

Zwecks Trainings und Optimierung der Engine finden die Entscheidungsergebnisse (inkl. der Ergebnisse aus der QA) im Rahmen des Kalibrierungsprozesses in der Decision-Engine (Fraud-Cockpit) Berücksichtigung.

Echtzeitbewertung unterstützt eine frühzeitige Verhinderung von Betrug.

?

Um die Entscheidungsqualität - möglichst wenige Fehlalarme mit einbezogen - zu optimieren, stellen sich drei Kernfragen:

1. **Haben wir die richtigen Regelwerke?**
2. **Haben wir die richtigen manuellen Prozesse?**
3. **Haben wir die richtigen Menschen mit Know-how, um die richtigen Entscheidungen zu treffen?**

„Der wichtigste Punkt im Rahmen der Betrugsprävention ist der Fokus auf das optimale Zusammenspiel von Tech, Analysen, Prozessen und Mitarbeitern. Keiner der Punkte allein wird einen umfassend wirkungsvollen Schutz gegen Betrug bieten können."

Michael Berghoff, Christ Juweliere

2.2.Nutzen eines effektiven Fraud Management Systems

Der Nutzen eines effektiven Fraud Management Systems besteht für den Kunden aus vier Elementen[29]:

Technisch	**System**
	• Bereitstellung eines Frühwarnsystems
	  • Echtzeitbewertung
	  • Regelwerk bestehend aus KI & MI
	  • Monitoring & Reporting
	• Maschinelles Lernen auf Basis vorhandener Datenbestände
		Daten
		• Gezieltes Nutzen der Daten für:
		  • Betrugsprävention
		  • Marketingaktivitäten
		  • Vertriebsaktivitäten
		• Erhöhung der Datenqualität

Prozessual	**Prozesse** • Erhöhung des Automatisierungsgrads • Reduzierung der Durchlaufzeiten • Erhöhung der Prozess- und Entscheidungsqualität	**Organisation** • Konzentration auf Kerngeschäft • Mittelfristige Kostenersparnis durch effizienten Ressourceneinsatz • Reduzierung von Betrugsrisiken und Verbesserung der Conversion Rate • Gewinne schützen • Erhöhtes Verständnis der Kundenbedürfnisse • Gezielte personalisierte Marketing/ Vertrieb Aktivitäten • Besseres Knowledge Management

[29] Quelle: Eigene Darstellung.

2.3.Beispielhaftes Fraud Cockpit

Das Fraud Cockpit besteht aus vier Bestandteilen:

- Rule-Engine (eine Softwarekomponente, die als Bestandteil eines Business-Rule-Management-Systems (BRMS) eine effiziente Ausführung von Geschäftsregeln ermöglicht)
- Reporting, bzw. Management Dashboard
- QA (Qualitäts-Absicherung)
- Auffälligkeitenliste (Arbeitsfläche für Fraud-Analysten)

Auszug Fraud Cockpit:

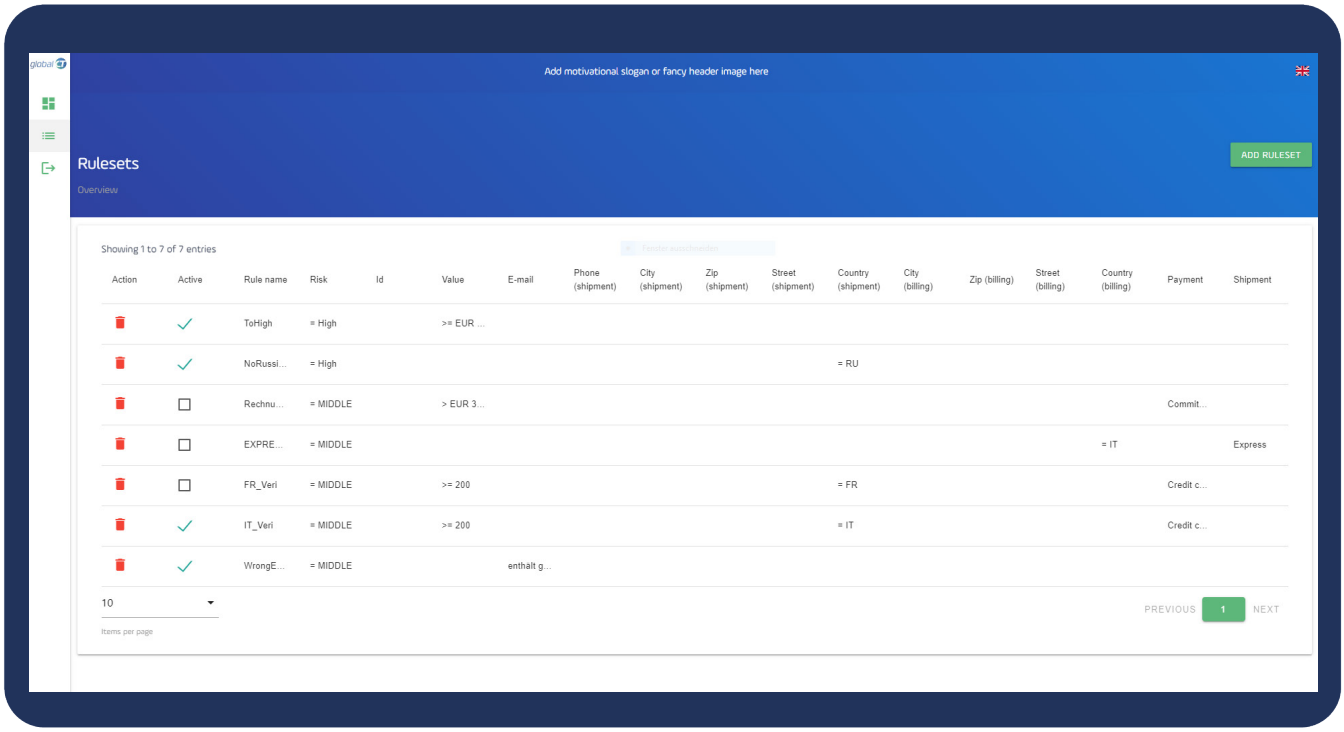


Abbildung 3 - Rule-Engine Beispiel[30]

In der Rule-Engine werden die Regelwerke für die weiteren Prüfungsprozesse implementiert. Die Regelwerke bewerten, ob eine Bestellung als gut oder verdächtig eingestuft wird. Die Regelwerke können zu jeder Zeit angepasst werden, um schnell auf eine mögliche Betrugswelle reagieren zu können.

Es gibt beim Akzeptieren oder Ablehnen einer Bestellung drei automatisierte Aktionen:

1. automatische Akzeptierung
2. sofortige Ablehnung
3. weitere Überprüfung durch den Fraud-Analysten in der Checkliste

[30] Quelle: Eigene Darstellung.

Manuelle Betrugsprüfung – unmittelbare Prüfung und Freigabe oder ggf. Storno der Verdachtsfälle

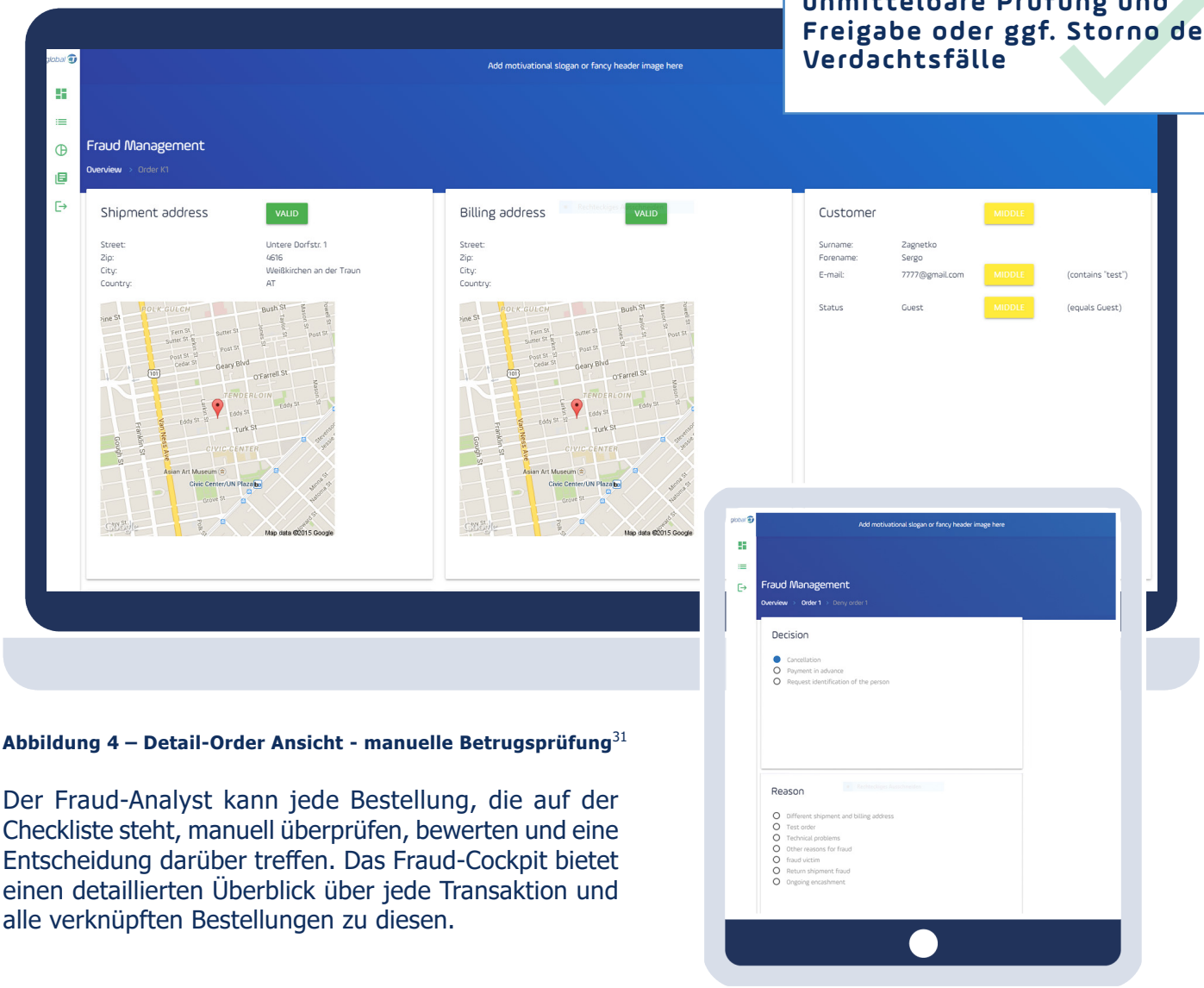


Abbildung 4 – Detail-Order Ansicht - manuelle Betrugsprüfung[31]

Der Fraud-Analyst kann jede Bestellung, die auf der Checkliste steht, manuell überprüfen, bewerten und eine Entscheidung darüber treffen. Das Fraud-Cockpit bietet einen detaillierten Überblick über jede Transaktion und alle verknüpften Bestellungen zu diesen.

[31] Quelle: Eigene Darstellung.

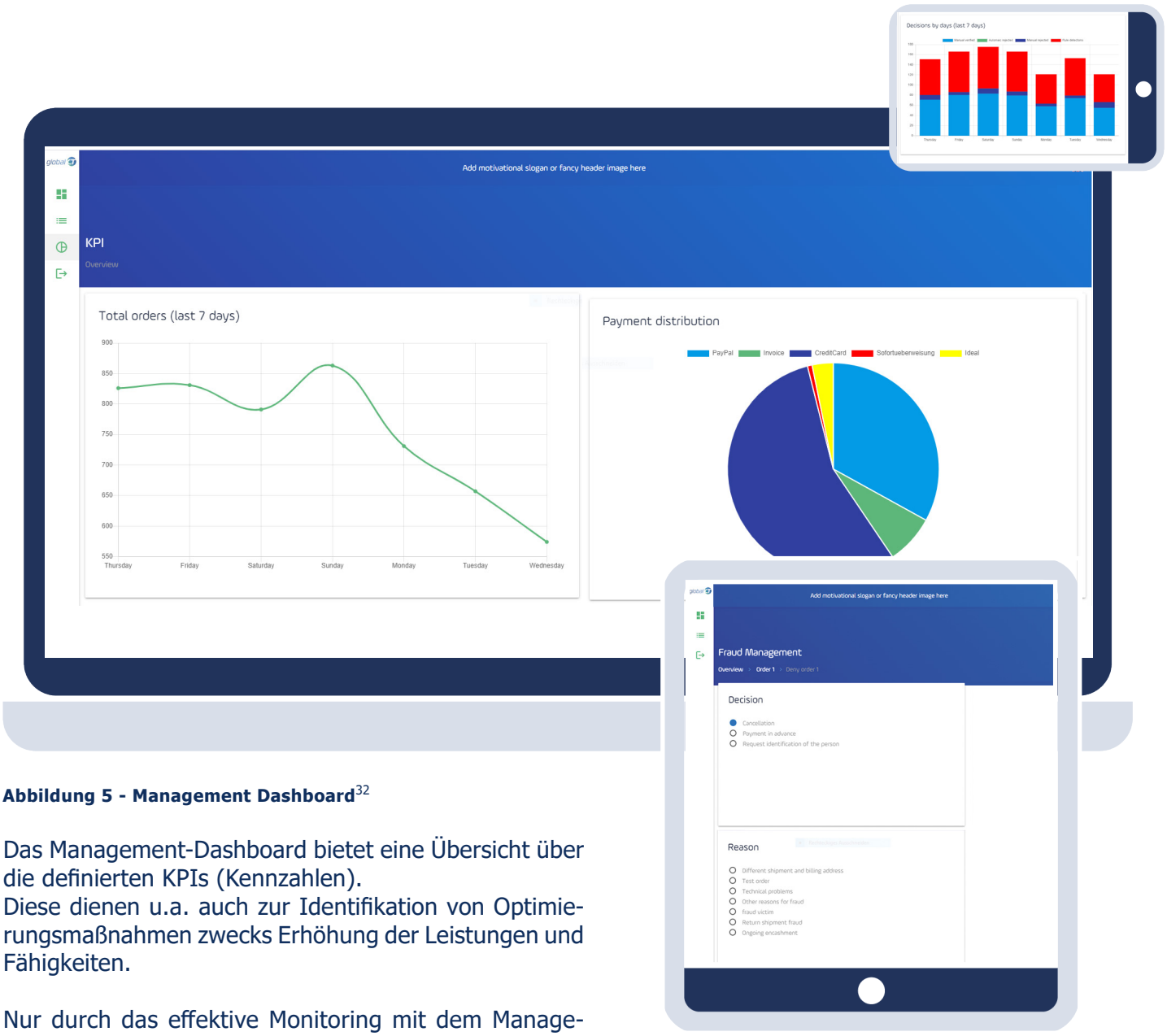


Abbildung 5 - Management Dashboard[32]

Das Management-Dashboard bietet eine Übersicht über die definierten KPIs (Kennzahlen).
Diese dienen u.a. auch zur Identifikation von Optimierungsmaßnahmen zwecks Erhöhung der Leistungen und Fähigkeiten.

Nur durch das effektive Monitoring mit dem Management-Dashboard/Reporting wird die Qualität des Fraud-Managements insgesamt gesichert und kontinuierlich verbessert.

[32] Quelle: Eigene Darstellung.

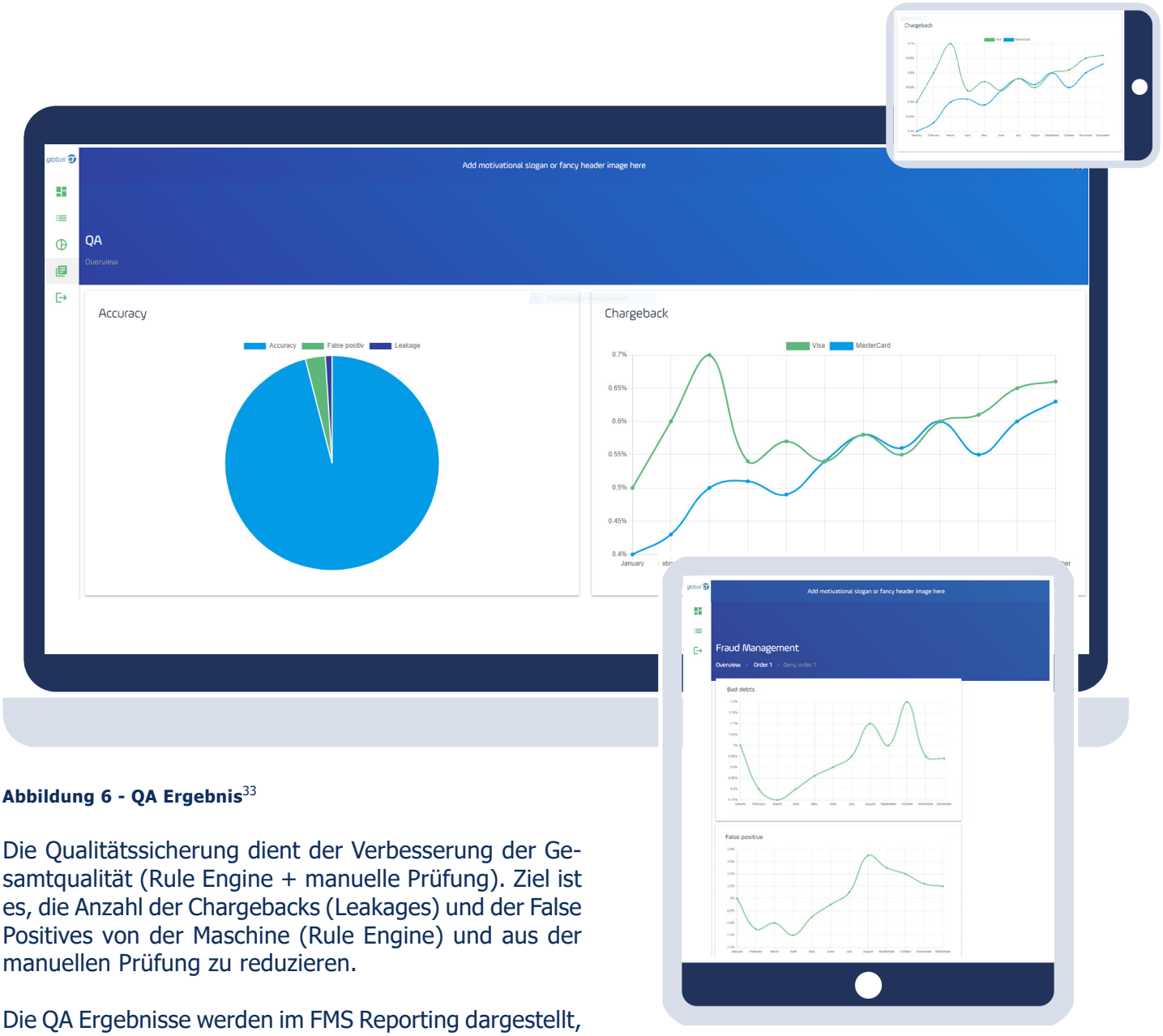


Abbildung 6 - QA Ergebnis[33]

Die Qualitätssicherung dient der Verbesserung der Gesamtqualität (Rule Engine + manuelle Prüfung). Ziel ist es, die Anzahl der Chargebacks (Leakages) und der False Positives von der Maschine (Rule Engine) und aus der manuellen Prüfung zu reduzieren.

Die QA Ergebnisse werden im FMS Reporting dargestellt, damit der Kalibrierungsprozess transparenter dargestellt wird und somit eindeutig wird, wie dieser funktioniert.

[33] Quelle: Eigene Darstellung.

3.FAZIT

Das kontinuierliche Fortschreiten der Digitalisierung und Technisierung im E-Commerce-Sektor öffnet Betrügern neue Einfallstore. Jeder Betrugsfall kann erhebliche finanzielle und rufschädigende Auswirkungen haben. Vor diesem Hintergrund ist es für Unternehmen unerlässlich, dieser Bedrohung proaktiv entgegenzutreten und ein effektives Fraud Management System in ihren Organisationen zu etablieren. Hierbei ist der Einsatz von KI und damit die Zusammenführung datengetriebener (Predictive Analytics) und technologiegetriebener (Fraud Cockpit) Ansätze mit dem Faktor Mensch maßgeblich. Die Basis dafür bilden die Daten, die hochskalierbar und immer verfügbar sein müssen. Predictive Analytics sorgt für die frühzeitige Erkennung der Betrugsfälle. Kombiniert mit einem dynamischen Lernprozess (Machine Learning), ermöglicht das effektive Fraud Cockpit eine Echtzeitbewertung durch Fraud-Analysten.

Trotz aller automatisierten Ansätze bleibt der Mensch entscheidend für den Erfolg in der Betrugsprävention. Die Leistungsfähigkeit und Qualität der KI hängen maßgeblich von den Bewertungen der Fraud-Analysten ab, deren traditionelle Rolle (100-Prozent-Prüfung) sich allerdings verändert. Neben der Transaktionsanalyse und Entscheidungsfindung begleitet der Fraud Analyst federführend den Kalibrierungsprozess und damit das Training der KI. In der Folge werden die automatischen Fraud Regelwerke kontinuierlich geschärft und aktualisiert.

Der kombinierte Einsatz von künstlicher sowie menschlicher Intelligenz sichert Gewinne, erhöht die Sicherheit und erleichtert die Compliance, unterstützt bei der Automatisierung von Arbeitsabläufen, steigert die Produktivität, verbessert die Customer Experience und ermöglicht es, sowohl Zeit als auch Kosten zu sparen. Die Anreicherung der KI mit weiteren Daten kann eine 360°-Rundumsicht auf die Kunden ermöglichen wodurch Unternehmen mit Blick auf Marketing- und Vertriebsaktivitäten Wettbewerbsvorteile generieren können. Hierbei sind jedoch die datenschutzrechtlichen Schranken zwingend zu beachten.

4. ÜBER DIE AUTORIN

Lu Liu, Senior Business Analyst
l.liu@globalct.com
https://globalct.com

Lu Liu ist Senior Business Analyst im Bereich Fraud und Risiko Management mit speziellem Fokus auf E-Commerce Finanzdienstleistungen. Ihr Schwerpunkt liegt auf der Entwicklung und Umsetzung von digitalen Risiko- und Fraud-Management-Produkten sowie die Einführung von Payment-, Fraud und Finanzdienstleistungen.

Auf Basis ihrer über zehnjährigen Erfahrung aus renommierten Beratungshäusern begleitet Frau Liu Kunden im Bereich der Betrugsprävention / Fraud Management von der Konzeptionierung, Produktentwicklung und Kundenbetreuung bis hin zum Fraud-Regelwerke Design, manuellen Prüfungsprozessen und Gestaltung von KPI-Reporting.

Auszug bisheriger Kunden von Lu Liu:
Apple Inc., Adidas, Converse (Nike), LEVIS, DIESEL, Bang & Olufsen, Versace, Hugo Boss, ESPRIT

Quellenverzeichnis

Agrawal.A (2018): Prediction Machines: The Simple Economics of Artificial Intelligence.

Crowe Global (2019): Fraud costs the global economy over US$5 trillion, URL: https://kurzelinks.de/ik5o (Stand: 09.03.2021).

Buchmann.T (2019): Whitepaper Digitalisierung der öffentlichen Verwaltung.

Experian plc (2018): The 2018 Global Fraud and Identity Report, Exploring the links between customer recognition, convenience, trust and fraud risk, URL: https://kurzelinks.de/g6wp (Stand: 08.02.2021).

Groeneveld, J. (2020): „Das ist kriminell": Der Chef der Bundesagentur für Arbeit droht Firmen, die bei Kurzarbeitergeld betrügen, Konsequenzen an – und die Linken wollen sogar Gefängnisstrafen, URL: https://kurzelinks.de/jclo (Stand: 08.02.2021).

Halbach, A. (2020): Corona-Hilfen - „Es gibt vermehrt Hinweise auf Betrug", URL: https://kurzelinks.de/dque (Stand: 08.02.2020).

JP Morgan (2021): 2021 AFP Payments Fraud and Control Survey, URL: https://kurzelinks.de/lx6e (Stand: 07.05.2021).

LexisNexis Risk Solutions (2018): 2018 True Cost of FraudSM Study, URL: https://kurzelinks.de/g9hh (Stand: 08.02.2021).

LexisNexis Risk Solutions (2020): 2020 True Cost of FraudSM Study.

Luber. S (2019) Was ist CRISP-DM? URL: https://kurzelinks.de/bzd1 (Stand. 17.03.2021).

Meier, J. (2020): Pressemitteilung – Betrugsversuche im eCommerce nehmen zu und verändern sich stetig, URL: https://kurzelinks.de/m22w (Stand: 08.02.2021).

Morrow, S.; Maynard, M (2020): Online Payment Fraud: Emerging Threats, Segment Analysis & Market Forecasts 2020-2024, URL: https://kurzelinks.de/kizk (Stand: 08.02.2021).

Nehls, N.; Otto, Michael (2015): Whitepaper – Anti-Fraud-Management, Wirtschaftskriminelle Handlungen zu Lasten von Finanzinstituten effektiv vermeiden, URL: https://kurzelinks.de/82z8 (Stand: 10.02.2021).

o. V. (2015): SAS® Fraud Management - Real-time scoring of all transactions for fast, accurate fraud detection, URL: https://kurzelinks.de/s9vh (Stand: 10.02.2021).

o. V. (2020): Online Merchant Perspectives – Fraud & Payment Survey 2020, URL: https://kurzelinks.de/votc (Stand: 08.02.2021).

o. V. (o. J.): Statista Marktprognose – eCommerce, URL: https://kurzelinks.de/tgfo (Stand: 09.03.2021).

o. V. (o. J.): Predictive Analytics - What it is and why it matters, URL: https://kurzelinks.de/rdwg (Stand: 15.03.2021).

o. V. (o. J.): Statista statistics – Retail e-commerce sales worldwide from 2014 to 2023, URL: https://kurzelinks.de/95p4 (Stand: 08.02.2021).

o. V. (o. J.): Our Process: Agile Data Science URL: https://kurzelinks.de/o7hi (Stand: 17.03.2021).

Statista (2021) eCommerce Deutschland URL: https://kurzelinks.de/zc3j (Stand: 07.05.2021).

Schuchter. A (2017): Fraud Management – Der vollständige Guide, URL: https://kurzelinks.de/yni6 (Stand: 08.02.2021).

Siller. H. (2018): Fraud - Definition: Was ist „Fraud"? URL: https://kurzelinks.de/ukvu (Stand: 09.02.2021).