LexisNexis®
RISK SOLUTIONS

Die wahren Kosten des

Betrugs in Deutschland

Im Rahmen einer weltweiten Online-Umfrage befragte Forrester **1.845** leitende Entscheidungsträger aus Finanzinstituten sowie Einzelhandels- und E-Commerce-Unternehmen. Ziel der Studie war es, den aktuellen Stand und die Herausforderungen im Bereich Betrug und Identitätsmanagement zu untersuchen. Zu den Umfrageteilnehmern aus Europa, dem Nahen Osten und Afrika (EMEA) gehören **541** leitende Entscheidungsträger aus **9** EMEA-Regionen.

Nachfolgend sind einige der wichtigsten Ergebnisse für Deutschland aufgeführt.

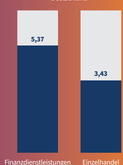
Da die Akzeptanz digitaler Dienste in Europa, dem Nahen Osten und Afrika (EMEA) zunimmt und das tägliche Leben immer stärker digitalisiert wird, sehen Cyberkriminelle mehr Möglichkeiten, sowohl Verbraucher als auch Unternehmen auszunehmen. **In der gesamten Region berichtet mehr als die Hälfte der befragten Unternehmen von einem Anstieg der Betrugsfälle (um 6 % oder mehr) in den letzten 12 Monaten, wobei 52 % der Betrugsfälle über digitale Kanäle verübt wurden.** Doch selbst wenn Unternehmen ihre Investitionen in Lösungen zur Betrugsprävention erhöhen, führen Kriminelle immer wieder neue, raffiniertere Betrugsmethoden ein (z. B. synthetische Identitäten), um diese Lösungen zu umgehen.

Die Auswirkungen auf die Unternehmen sind vielfältig. Berücksichtigt man Geldstrafen, Gebühren und den Aufwand für die Untersuchung betrügerischer Transaktionen, entstehen den Unternehmen Betrugskosten, die drei- bis fünfmal so hoch sind wie der tatsächliche Wert, der den Betrügern entgangen ist. Dabei sind die Auswirkungen auf das Kundenerlebnis noch gar nicht berücksichtigt: **71 % der Befragten sehen keine negativen Auswirkungen auf die Konversionsraten ihrer Kunden**.

Die wahren Kosten des Betrugs in Deutschland

Für Einzelhändler umfasst dies die Kosten für Gebühren und Zinsen sowie die Kosten für die Wiederbeschaffung verlorener/gestohlener Waren.

Mit den umfassenderen Vorschriften, die zusätzliche Ermittlungsbemühungen, höhere Arbeitskosten und die Haftung bei der Rückerstattung von Kunden erfordern, sind die Gesamtkosten des Betrugs für die Finanzinstitute noch höher.



Basis: 541 Entscheidungsträger aus dem gesamten EMEA-Raum mit Zuständigkeit für die Strategie zur Betrugsbekämpfung in ihrer jeweiligen Organisation
Quelle: Studie von Forrester Consulting im Auftrag von LexisNexis Risk Solutions, Juli 2023

Die wichtigsten Arten von Online-Betrug nehmen zu

Finanzdienstleistungen

1. Identitätsdiebstahl
2. Synthetischer Identitätsbetrug
3. Gefälligkeitsbetrug (Friendly/frivolous fraud)
4. Kartenprüfungsbetrug
5. Betrug bei mobilen Transaktionen

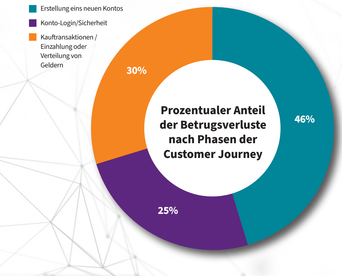
Einzelhandel

1. Bandenbetrug (Collusion fraud)
2. Gefälschte Bewertungen und Ratings
3. Verkaufsförderungsbetrug /Polizeimissbrauch (Nur Einzelhandel und E-Commerce)

Gestohlene und synthetische Identitäten tragen am stärksten zu Betrugsverlusten bei

Kriminelle machen sich die Beliebtheit des digitalen Bankings und des digitalen Handels zunutze, um mit gestohlenen oder künstlichen Identitäten neue Konten zu eröffnen.

Fast die Hälfte aller Verluste lässt sich auf die betrügerische Einrichtung neuer Konten zurückführen.



Mit den sich ständig weiterentwickelnden Trends und Bedrohungen Schritt halten

Die 5 größten Herausforderungen bei der Betrugsbekämpfung

1. Außerstandessein, Betrug bei neuen Transaktionsmethoden zu verwalten/verhindern
2. Mangel an spezialisierten Betrugspräventionsinstrumenten für internationale Bestellungen/ Transaktionen
3. Nicht fähig, zwischen legitimen menschlichen und bösartigen Bot-Transaktionen zu unterscheiden
4. Außerstandessein, auf dem Laufenden zu bleiben und sich gegen neue, ausgefeiltere Betrugsmethoden im Zahlungsverkehr zu schützen
5. Gleichgewicht zwischen Betrugsprävention und Kundenerlebnis

Fragmentierte Nutzung von Lösungen zur Identitäts- und Transaktionsüberprüfung

Erstellung eines neuen kontos	Konto-Login/ Sicherheit	Kauftransaktionen / Einzahlung oder Verteilung von Geldern
Geolokalisierung	Automatisierte Transaktionsbewertung	Geolokalisierung
Browser-/Malware-Überwachung	Kundenauthentifizierung mit verhaltensbiometrischer Technologie	Browser-/Malware-Überwachung
Geräte-ID/Geräte-Fingerprinting	Geolokalisierung	Automatisierte Transaktionsbewertung

Laden Sie die LexisNexis **EMEA True Cost of Fraud Study** herunter, um mehr darüber zu erfahren, wie man ein Gleichgewicht zwischen Betrugsprävention und nahtlosem Kundenerlebnis herstellen kann.

Studie herunterladen

LexisNexis®
RISK SOLUTIONS