

Da der digitale Wandel im Finanzdienstleistungs- und Einzelhandelssektor immer schneller voranschreitet, zeigt der jüngste LexisNexis® True Cost of Fraud™- Bericht, dass Cyberkriminelle eine größere Anzahl von Zahlungsmethoden angehen und die Betrugskosten in neue Höhen treiben.

Der Deutschland LexisNexis® Fraud Multiplier™ ist in 2021 gestiegen um

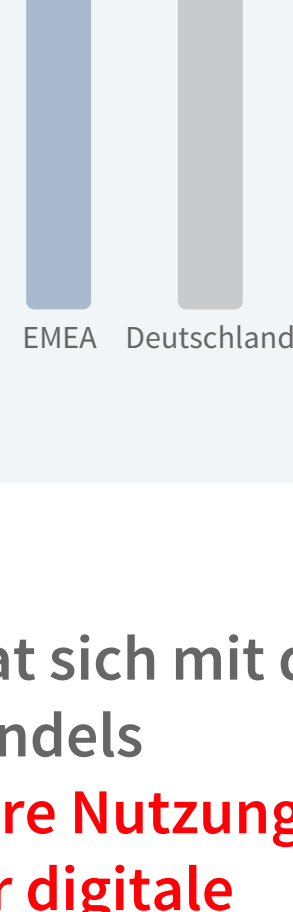
12.3%

im Vergleich zu 2019



Jede betrügerische Transaktion kostet im Durchschnitt das **3,38-fache** des verlorenen Transaktionswertes

LexisNexis Fraud Multiplier™



Das Verhalten der Verbraucher hat sich mit der Beschleunigung des digitalen Wandels verändert, u. a. durch eine **stärkere Nutzung von Fernabsatzkanälen und mehr digitale Zahlungsmöglichkeiten**.

- Die Nutzung **mobile/digital wallets** macht einen ähnlichen Anteil am Transaktionsvolumen aus wie Kredit- und/oder Debitkarten.

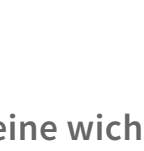


Nutzung von mobile/ digital wallets hat zugenommen um

50%

seit 2019.

- E-Commerce-Händler setzen zunehmend auf einen **Omni-channel-Ansatz**, indem sie entweder eigene Filialen eröffnen oder Partnerschaften mit Einzelhändlern für die Abholung eingehen.

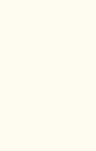


Das durchschnittliche Transaktionsvolumen über den mobilen Kanal ist gestiegen um

50%

seit 2019.

- Bei Transaktionen über mobile Kanäle sind **Apps** eine wichtige Methode, die von den Verbrauchern genutzt wird.



Die Nutzung des mobilen Kanals über die App eines Drittanbieters hat zugenommen um

67%

seit 2019.

Der digitale Wandel bietet **Betrügern neue Möglichkeiten** und trägt zum Anstieg der Betrugskosten bei.

Die monatlichen bössartigen Bot-Angriffe haben um

47%

zugewonnen im Vergleich zu vor 12 Monaten

Unser neuester Cybercrime Bericht, der auf Kundendaten in unserem Lexis Nexis® Digital Identity Network® basiert, zeigt, dass Bot-Angriffe zurückgegangen sind um

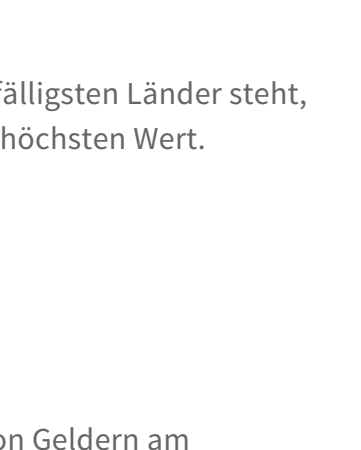
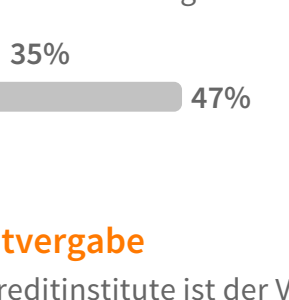
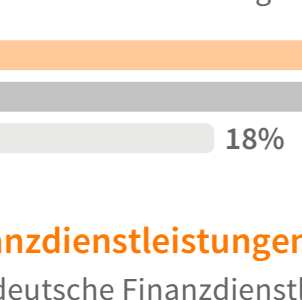
9%

Jahr für Jahr in Deutschland

- Transaktionen, die bössartige Bot-Angriffe sind, in Prozent

10% EMEA **9%** Deutschland

- Im Vergleich zu vor 12 Monaten haben sich die monatlichen bössartigen Bot-Angriffe...



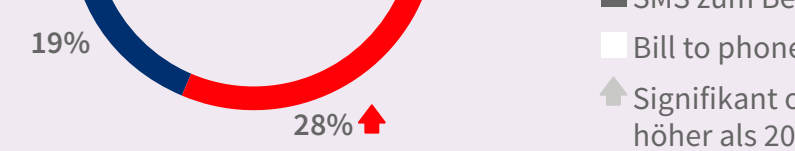
Die **betrugsanfälligste Phase** der Customer Journey

Die für Betrug am **MEISTEN** anfällige Phase der Customer Journey

Einrichtung eines neuen Kontos Kauftransaktionen/Verteilung von Geldern Kontoanmeldung

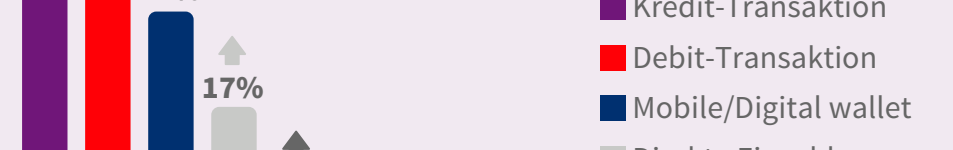
Einzelhandel & e-Commerce

Obwohl die Einrichtung neuer Konten an zweiter Stelle der betrugsanfälligsten Länder steht, hat Deutschland im Vergleich zu den anderen EU-Mitgliedstaaten den höchsten Wert.



Finanzdienstleistungen und Kreditvergabe

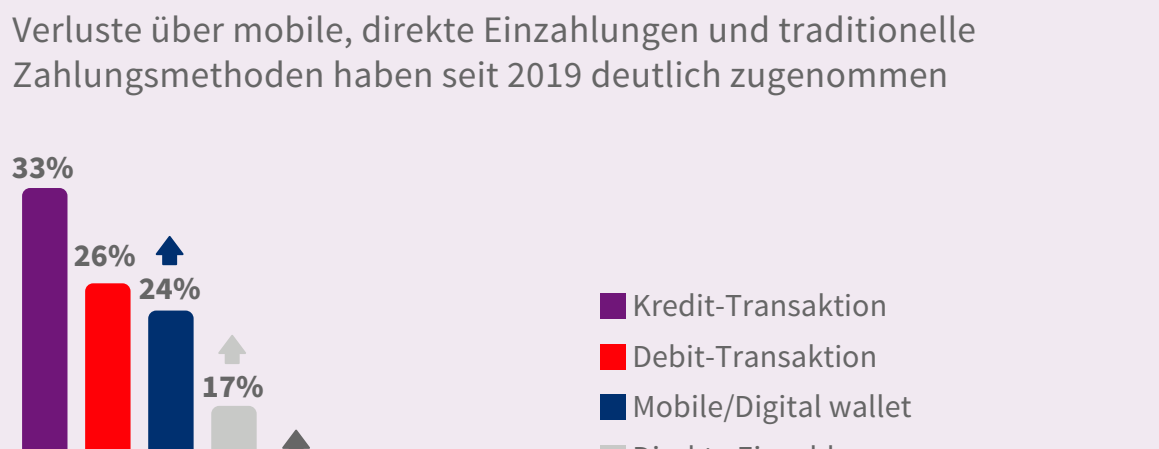
Für deutsche Finanzdienstleister und Kreditinstitute ist der Vertrieb von Geldern am anfälligsten für Betrug - höher als im EMEA-Durchschnitt.



Während mobile Apps und Browser nach wie vor einen beträchtlichen Teil der Betrugskosten im mobilen Kanal ausmachen, tragen auch **kontaktlose Bezahlmethoden** zu Betrugsverlusten bei.

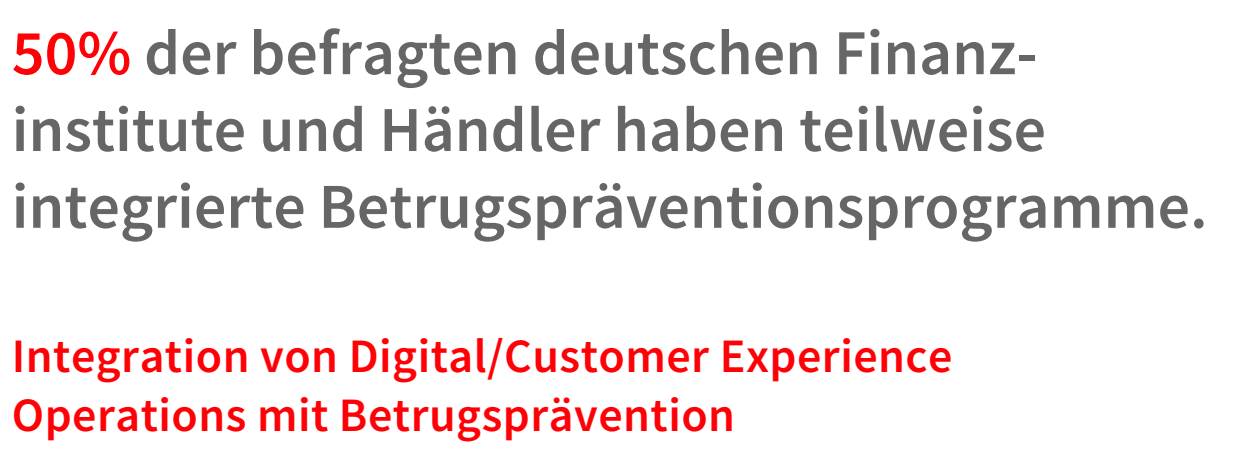
Betrugskosten nach mobilen Kanälen

Betrüger haben ihre Angriffe auf den mobilen Kanal intensiviert. Die Betrugskosten durch mobile Apps von Drittanbietern und kontaktlose Käufe sind deutlich höher als 2019



Verteilung von Verlusten nach Zahlungsmethode, in Prozent

Verluste über mobile, direkte Einzahlungen und traditionelle Zahlungsmethoden haben seit 2019 deutlich zugenommen



50% der befragten deutschen Finanzinstitute und Händler haben teilweise integrierte Betrugspräventionsprogramme.

Integration von Digital/Customer Experience Operations mit Betrugsprävention

Vollständig integriert

32%

Teilweise integriert

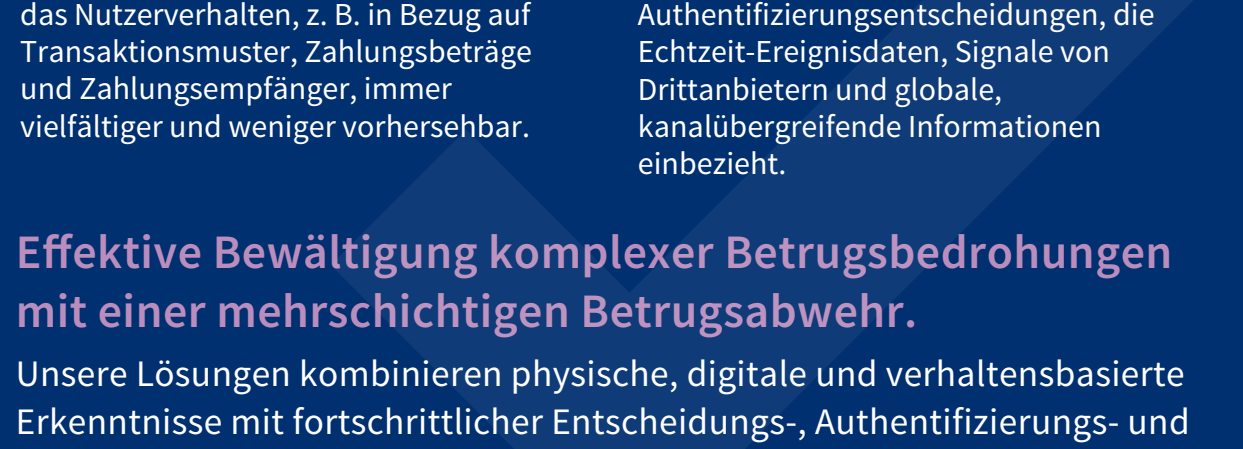
50%

Netz: Nicht integriert

18%

Bewährte Praktiken zur Betrugsprävention:

Es ist ein Lösungsansatz mit mehreren Ebenen erforderlich, der auf jede Phase der Customer Journey und jeden Transaktionskanal zugeschnitten ist.



- ✓ Ein einziger Schutz reicht nicht mehr aus und führt zu einem einzigen Ausfallpunkt.
- ✓ Da die Verbraucher ihre Transaktionen standort-, geräte- und länderübergreifend abwickeln, wird das Nutzerverhalten, z. B. in Bezug auf Transaktionsmuster, Zahlungenbeträge und Zahlungsempfänger, immer vielfältiger und weniger vorhersehbar.

- ✓ Darüber hinaus ist jede Phase der Customer Journey eine einzigartige Interaktion, die unterschiedliche Arten der Identitätsüberprüfung, Daten und Lösungen erfordert, um Ihre Kunden hereinzulassen und die Betrüger fernzuhalten.
- ✓ Ein hochschichtiger, starker Authentifizierungsschutz ist erforderlich. Dazu gehört eine einzige Plattform für Authentifizierungsentscheidungen, die Echtzeit-Ereignisdaten, Signale von Drittanbietern und globale, kanalübergreifende Informationen einbezieht.

Effektive Bewältigung komplexer Betrugsbedrohungen mit einer mehrschichtigen Betrugsabwehr.

Unsere Lösungen kombinieren physische, digitale und verhaltensbasierte Erkenntnisse mit fortschrittlicher Entscheidungs-, Authentifizierungs- und verhaltensbiometrischer Technologie, um Ihr Unternehmen in die Lage zu versetzen, Betrug zu erkennen.

Laden Sie unsere vollständige **True Cost of Fraud™ - EMEA-Ausgabe** herunter, um einen tieferen Einblick zu erhalten und zu sehen, wie Deutschland im Vergleich zu anderen untersuchten Ländern abschneidet.