Building Trust in a World of Deception

Experian research conducted by Forrester Consulting

Willkommen zum Experian Fraud Report 2026

In den letzten Jahren hat sich die Betrugsbedrohung erheblich ausgeweitet. Sie ist heute stärker organisiert und industrialisiert, unterstützt durch immer leistungsfähigere Werkzeuge, die zu einem massiven Anstieg von Umfang und Raffinesse der Angriffe führen.

Ganze Regionen haben sich zu regelrechten „Scam-Fabriken" entwickelt, die weltweit Menschen ins Visier nehmen. Hinzu kommt die wachsende Beteiligung staatlich sanktionierter krimineller Organisationen an koordinierten Angriffen – einige Experten sprechen bereits vom „goldenen Zeitalter des Betrugs".

Die Bewältigung dieser Herausforderung erfordert enge Zusammenarbeit – denn gemeinsame Anstrengungen sind deutlich wirksamer als isolierte Maßnahmen.

Organisationen, die Teil des Experian-Netzwerks von Betrugskonsortien sind, verzeichnen oft eine signifikante Reduzierung der Betrugsverluste, indem sie auf die kollektive Intelligenz zurückgreifen, die innerhalb der Gruppe geteilt wird.

Unternehmen müssen heute auf modernste Technologien zur Betrugsprävention setzen. KI ist dabei ein entscheidender Treiber: Sowohl Machine Learning als auch Generative AI eröffnen neue Möglichkeiten, Betrüger schneller zu identifizieren, sich flexibel an Veränderungen anzupassen und Betrugssysteme effizienter zu steuern – zum Schutz von Unternehmen und Kunden.

In der diesjährigen Studie, die in Zusammenarbeit mit Forrester Consulting durchgeführt wurde, haben wir knapp 1.000 Entscheidungsträger im Bereich Betrug aus neun Ländern nach ihren Ansichten zu den großen Trends gefragt, die die Betrugsprävention beeinflussen. Ich bin sicher, dass ihre gesammelten Erkenntnisse Ihnen helfen werden, Ihre Betrugsstrategie für das kommende Jahr zu verfeinern.

Und wann immer Sie bereit sind, ein Gespräch über unsere End-to-End-Plattform zur Betrugsprävention zu beginnen, freut sich unser globales Team aus erfahrenen Beratern darauf, mit Ihnen zu sprechen.

SHAIL DEEP
COO Experian EMEA & APAC

Inhalt

TEIL 1

Herausforderungen und Prioritäten

Bericht von der Front

Erfahren Sie, wie sich Betrugsangriffe branchenübergreifend entwickelt haben – und welche Betrugsarten am schwersten zu erkennen sind.

Die größten Betrugsherausforderungen

Welche Faktoren erschweren die Betrugsprävention im kommenden Jahr? Und wie verändert GenAI die Bedrohungslage?

Prioritäten für das kommende Jahr

Welche strategischen Schwerpunkte stehen in den nächsten zwölf Monaten im Fokus?

TEIL 2

Technologiegestützte Lösungen

Warum Machine Learning im Kampf gegen Betrug unverzichtbar ist

Welche Vorteile ML bietet – und warum einige Organisationen noch zögern.

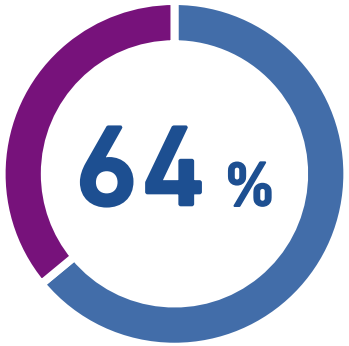
GenAI-Assistenten und digitale Identitäts-Wallets

Wie GenAI-Assistenten das Betrugsmanagement optimieren und digitale Identitäts-Wallets die Authentifizierung verändern.

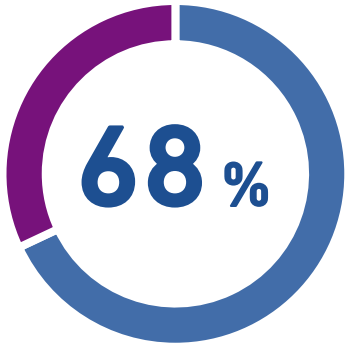
Der Wandel zu Shared Fraud Intelligence

Warum Zusammenarbeit in Betrugskonsortien die Zukunft der Prävention bestimmt.

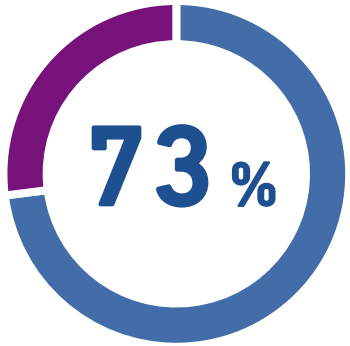
Momentaufnahme der wichtigsten Ergebnisse



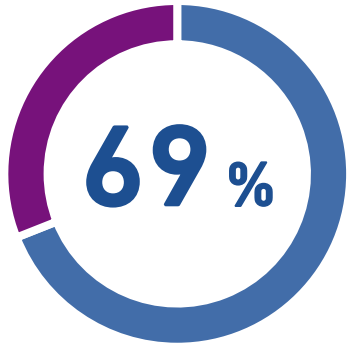
berichten von gestiegenen Betrugsverlusten gegenüber dem Vorjahr.



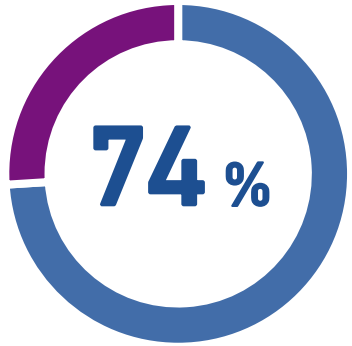
bestätigen, dass ihr aktueller Technologie-Stack nicht ausreicht, um der sich schnell entwickelnden Betrugsbedrohung standzuhalten.



sind daran interessiert, in passive Betrugsprüfungen wie Verhaltens- und Gerätedaten zu investieren, um Reibungsverluste zu minimieren.



planen, Betrugsprävention und Kreditrisikobewertung in eine integrierte Risikomanagementstrategie einzubinden.



stimmen zu, dass die Mehrheit der Unternehmen in den nächsten drei Jahren Teil einer Gruppe für Shared Fraud Intelligence sein wird.

Basis: 979 leitende Entscheidungsträger im Bereich Betrug in EMEA & APAC
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

TEIL 1: Herausforderungen und Prioritäten

Bericht von der Front

Betrug ist heute schneller und günstiger umsetzbar als je zuvor. Die Kombination aus grenzüberschreitenden Cyberbedrohungen und GenAI-gestützten Angriffen hat Volumen und Komplexität massiv erhöht.

Laut einer aktuellen Studie haben sich Betrugssyndikate in Südostasien zum „mächtigsten kriminellen Netzwerk der modernen Ära" entwickelt, das jährlich 50–70 Milliarden US-Dollar mit einer Belegschaft von über 350.000 Personen erwirtschaftet. Darüber hinaus bieten „Fraud-as-a-Service"-Anbieter im Darknet eine wachsende Palette von Produkten an, um Betrüger mit den neuesten Werkzeugen und kriminellen Informationen auszustatten.

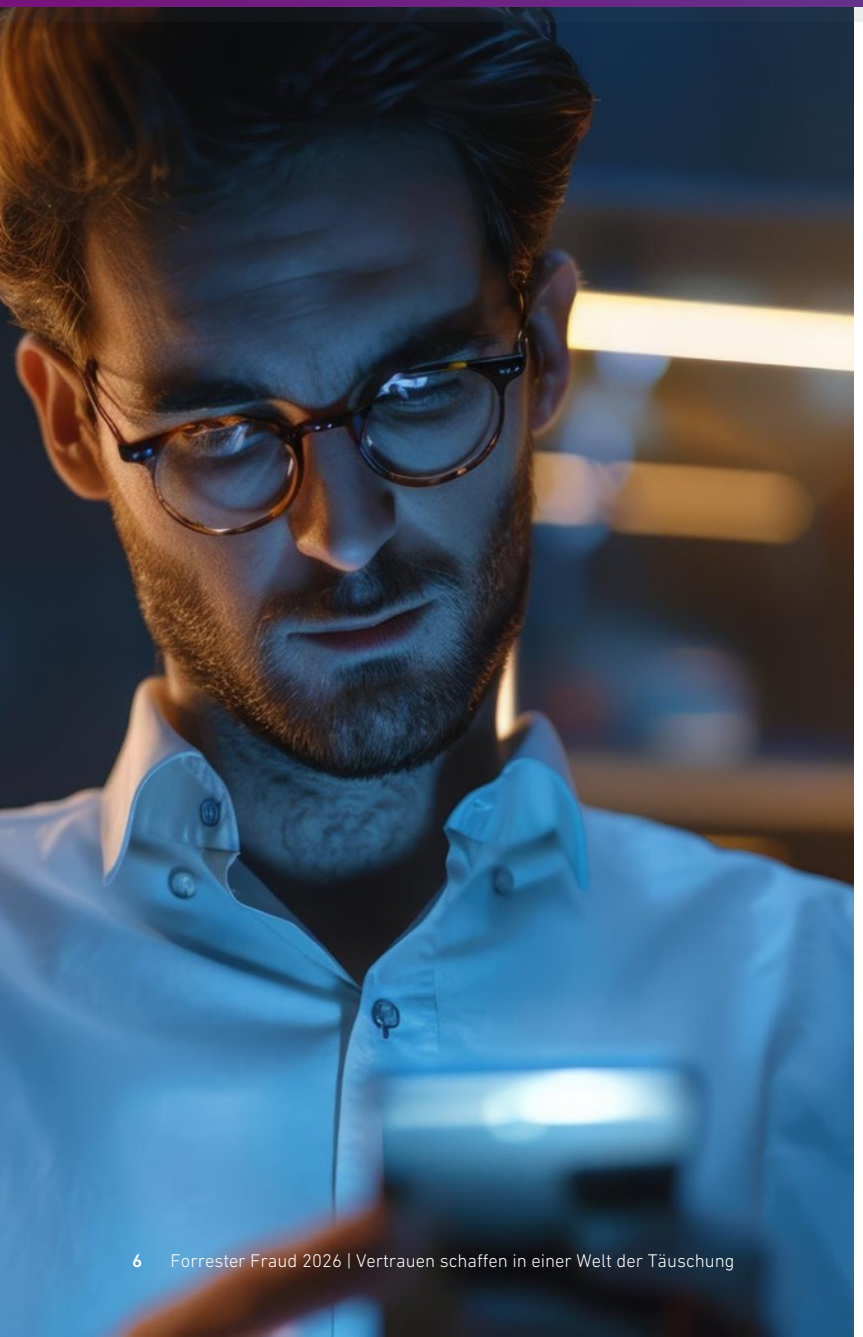
Unsere Untersuchung zeigt, dass diese Bedrohung Unternehmen weltweit betrifft, wobei **mehr als zwei Drittel (67 %) der Befragten 2026 mehr Betrugsangriffe erwarten als im Vorjahr, was einem Anstieg von 10 % gegenüber dem Vorjahr entspricht.**

Die Folgen sind deutlich: 64 % berichten von steigenden Betrugsverlusten und geben zu, dass ihre Organisation Mühe hat, mit der dynamischen Bedrohung Schritt zu halten. Die Auswirkungen dieses Betrugs-Tsunamis gehen über finanzielle Verluste hinaus, wie die 67 % zeigen, die zustimmen, dass Betrugsfälle dem Ruf ihrer Organisation schaden.

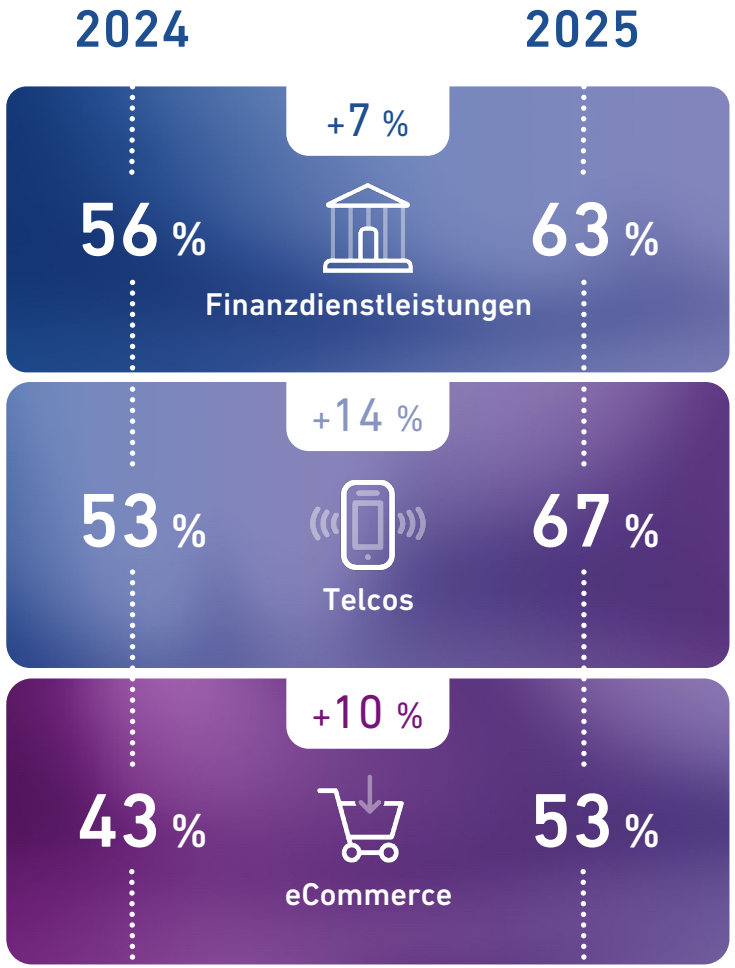
Welche Betrugsarten haben am stärksten zugenommen?

Branchenvergleich: Telcos verzeichnen den stärksten Anstieg – 67 % melden mehr Betrugsangriffe. Finanzdienstleister folgen mit 63 %, eCommerce liegt bei 53 %.

67 % **erwarten mehr Betrugsangriffe als im letzten Jahr**



Prozentsatz der Organisationen, die einen Anstieg der gesamten Betrugsangriffe melden (2024 vs. 2025)



Basis: 979 leitende Entscheidungsträger im Bereich Betrug in EMEA & APAC
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

Im Vergleich zum Vorjahr sind Social Engineering, Loyalitäts-/Prämienbetrug und Identitätsdiebstahl die am schnellsten wachsenden Bedrohungen für Finanzdienstleister und Telcos. Angesichts der Tatsache, dass GenAI zu einem leistungsstarken Hilfsmittel geworden ist, überrascht es nicht, dass Social Engineering auf dem Vormarsch ist. Auch Treueprogramme und Prämien geraten zunehmend ins Visier, da sie oft als weniger sicher gelten.

Die Identitätsüberprüfung ist zum wichtigsten Sicherheitsperimeter und zum Hauptziel von Betrügern geworden. Da legitime AI-Agenten zunehmend neben Bots und Deepfakes mit Websites interagieren, ist die Fähigkeit zur genauen Authentifizierung und Überprüfung der Kundenidentität von entscheidender Bedeutung.

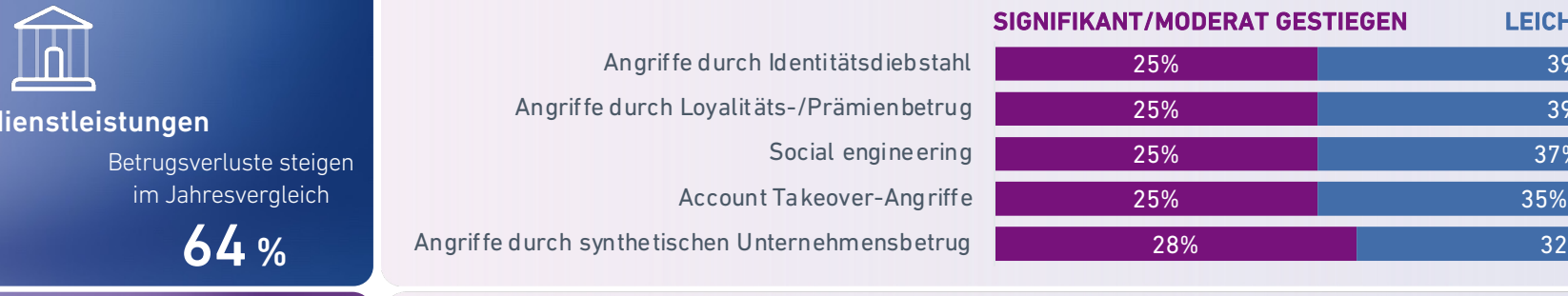
Im eCommerce haben Friendly Fraud und Rückerstattungsmissbrauch den größten Anstieg im Jahresvergleich gezeigt. Auch Angriffe mit synthetischen Identitäten nehmen zu, wenn auch in geringerem Umfang.

Anstieg der Betrugsarten im Jahresvergleich (nach Branche)

Finanzdienstleistungen

Anstieg der gesamten Betrugsangriffe: **63 %**

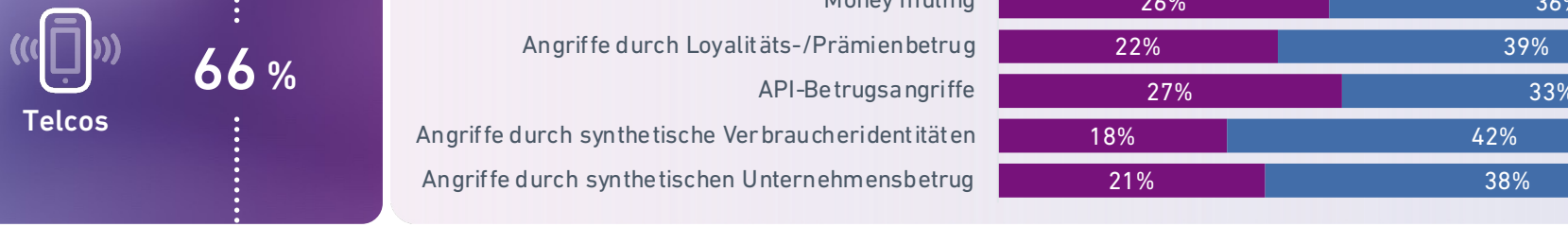
Betrugsverluste steigen im Jahresvergleich: **64 %**



Telcos

67 %

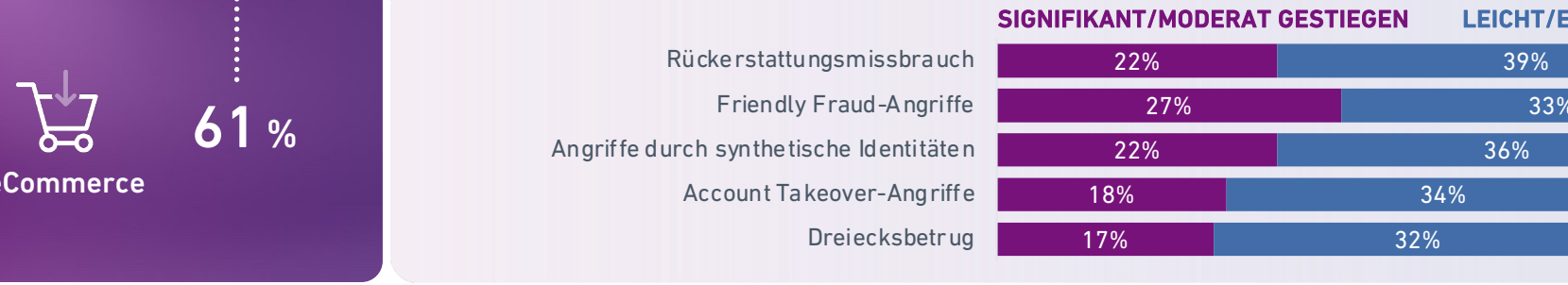
66 %



eCommerce

53 %

61 %



Basis: 979 leitende Entscheidungsträger im Bereich Betrug in EMEA & APAC
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

Welche Betrugsarten sind am schwierigsten zu erkennen und zu verhindern?

Unsere Studie zeigt:

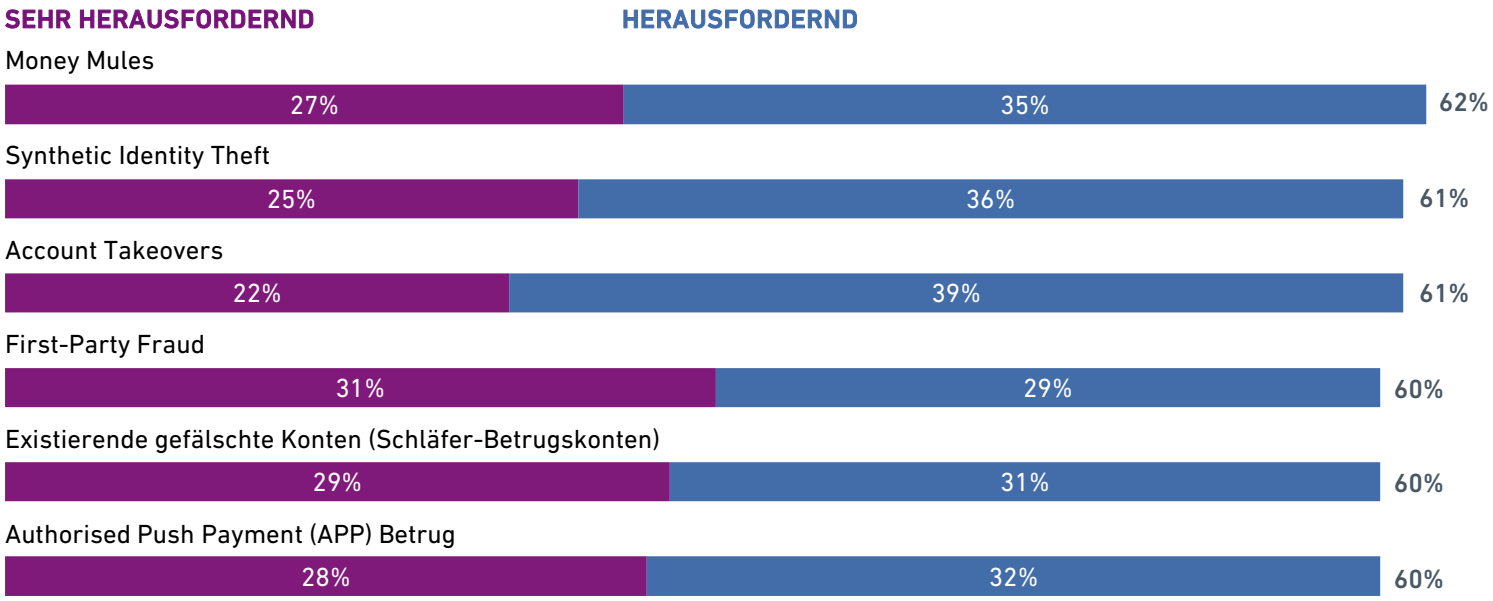
- Money Mules sind die größte Herausforderung
- Gefolgt von synthetischem Identitätsdiebstahl und Account Takeover

Diese Betrugsarten erfordern zusätzliche Signale wie Geräte- und Verhaltensdaten, um Muster zu erkennen

Traditionelle Authentifizierungsmethoden sind heute leicht durch GenAI-gestütztes Social Engineering und Darknet-Daten zu umgehen. Betrugsarten, die schwer zu identifizieren sind, können nur durch subtile Geräte- und Verhaltenssignale verhindert werden, die aufzeigen, wenn das normale Benutzerverhalten abgewichen ist. Nur 42 % der Unternehmen nutzen derzeit Gerätedaten, 39 % setzen Verhaltensbiometrie ein – ein Grund, warum diese Angriffe schwer zu verhindern sind.

Ohne fortschrittliche Tools steigt das Risiko, dass kompromittierte Zugangsdaten zu Systemzugriff führen. Darknet-Monitoring wird zunehmend unverzichtbar, um verfügbare Daten und neue Betrugstaktiken im Blick zu behalten.

Was sind die am schwierigsten zu erkennenenden und zu verhindernden Betrugsarten?



Basis: 979 leitende Entscheidungsträger im Bereich Betrug in EMEA & APAC
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

Die größten Herausforderungen bei der Betrugserkennung

Die drei Hauptprobleme, die die Fähigkeit von Organisationen zur Erkennung und Verhinderung von Betrug einschränken, basieren alle auf einem Mangel an Fähigkeiten. Gerätedaten und physische Biometrie werden als die wichtigsten fehlenden Fähigkeiten identifiziert; eng damit verbunden ist der Bedarf an AI/ML-Expertise, um diese Signale in genaue, zuverlässige Betrugsentscheidungen umzuwandeln.

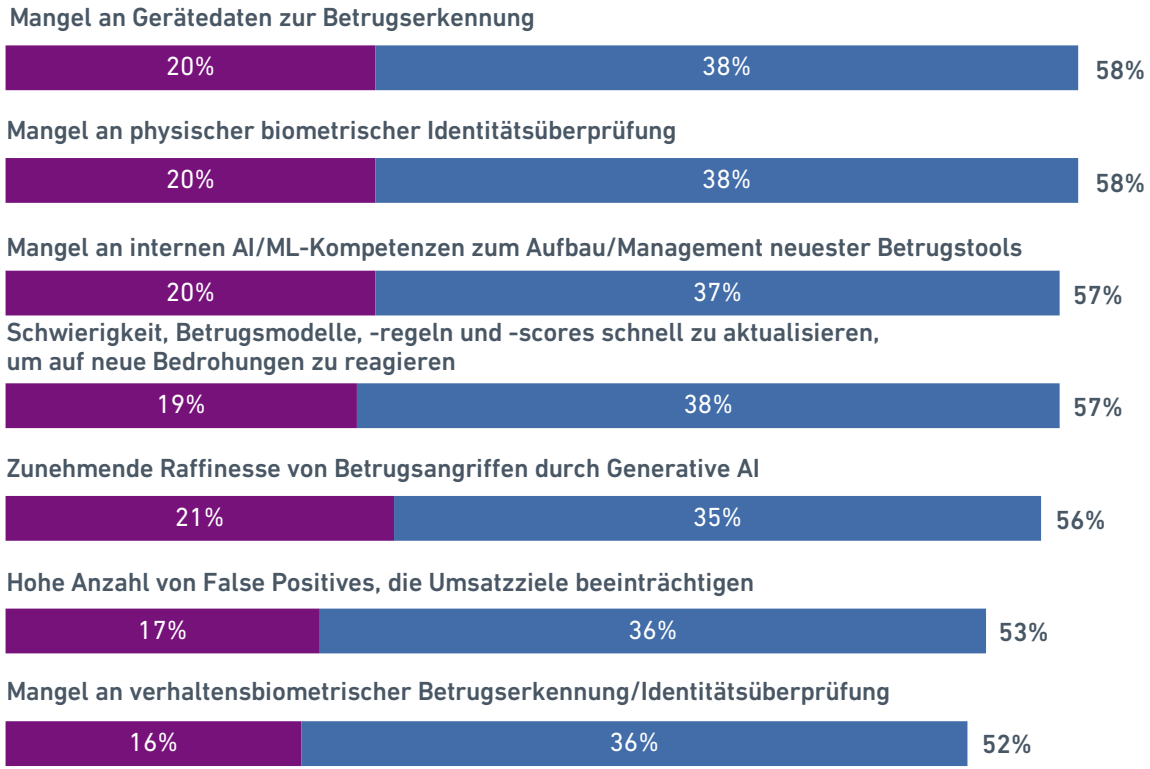
Kompetenzlücke:

Viele Unternehmen stecken in einem Dilemma: Ihre Systeme sind unzureichend, doch es fehlen Ressourcen und Know-how für die Einführung fortschrittlicher Tools. Die „Build vs. Buy"-Frage wird dringlicher, da Angriffe immer komplexer werden.

Unternehmen benötigen jetzt Lösungen – nicht erst in einem Jahr oder später (die Zeit, die eine interne Entwicklung in Anspruch nimmt).
Das Abwägen interner Kompetenzen und Fähigkeiten gegen eine wachsende Betrugsbedrohung ist entscheidend für zukünftiges Wachstum geworden. Es ist interessant festzustellen, dass fast drei Viertel (71 %) der Befragten angeben, dass sie mehr in Betrugstechnologie als in menschliche Betrugsanalysten investieren.

68 % bestätigen, dass ihr aktueller Technologie-Stack nicht ausreicht, um der dynamischen Bedrohung zu begegnen.

Top-Herausforderungen, die die Fähigkeit zur Betrugserkennung einschränken



Basis: 979 leitende Entscheidungsträger im Bereich Betrug in EMEA & APAC
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

Der GenAI-Betrugszug rollt weiter

GenAI ist die treibende Kraft hinter der aktuellen Betrugswelle: Sie verbindet riesige Datenmengen aus dem Darknet mit Hunderttausenden von Betrügern. Dark LLMs wie WolfGPT und WormGPT machen es jedem mit Internetzugang leicht, sich Wissen für unterschiedlichste Betrugsangriffe anzueignen.

Die Qualität gefälschter Dokumente und Deepfake-Bilder hat sich rasant verbessert. 64 % der Befragten bestätigen, dass ihre aktuellen KYC- und Identitätsprüfungen nicht darauf ausgelegt sind, GenAI-generierte Dokumente zu erkennen.

Die Kombination aus echten Kundendaten und synthetischen Bildern macht die Identifizierung noch komplexer. Da leistungsfähige Tools immer günstiger und leichter verfügbar werden, verschärft sich das Problem weiter. Tatsächlich **stimmen 60 % zu, dass wir beim AI-gestützten Betrug erst die Spitze des Eisbergs gesehen haben.**

AI

66% **der Betrugsexperten stimmen zu, dass GenAI die größte Herausforderung für die Betrugsprävention aller Zeiten darstellt**

Ein Beispiel für diese Entwicklung: Deepfakes können inzwischen sogar Herzschlag-Signale imitieren. Bis vor Kurzem galt die Hauttonvariation als verlässliches Erkennungsmerkmal – heute wird selbst dieses Signal täuschend echt nachgebildet.

Es besteht kein Zweifel, dass das Aufkommen von GenAI einen Wendepunkt in der Betrugsprävention darstellt. Die Grenze zwischen Realität und Fälschung ist verschwommen, und die Konsequenzen sind ungewiss. 60 % stimmten zu, dass ihre Betrugsverluste seit GenAI signifikant gestiegen sind. Ein ähnlicher Prozentsatz (58 %) gibt jedoch zu, dass sie Schwierigkeiten haben zu erkennen, ob GenAI an einem Angriff beteiligt war, und es daher schwierig finden, die Auswirkungen zu quantifizieren.

Sollten Deepfakes illegal sein?

61 % der Befragten befürworten ein generelles Verbot zum Schutz der Gesellschaft. Zwar arbeiten Gesetzgeber weltweit an Regelungen, doch bisher fehlt ein klarer Rechtsrahmen – die Bedrohung bleibt nahezu unkontrolliert.

Dänemark ist eines der wenigen Länder, das auf dieses Problem mit Dringlichkeit reagiert hat, indem es kürzlich Änderungen am Urheberrecht vorgeschlagen hat, um sicherzustellen, dass jeder das Recht am eigenen Körper, den eigenen Gesichtszügen und der eigenen Stimme hat.

Italien hat ebenfalls entschlossene Maßnahmen ergriffen, indem es die Erstellung und Verbreitung schädlicher Deepfakes im Rahmen seines neuen nationalen AI-Gesetzes offiziell zur Straftat erklärt hat. Diese Gesetzgebung, die erste ihrer Art in der EU, sieht Haftstrafen für Personen vor, die unrechtmäßig AI-generierte oder manipulierte Inhalte, einschließlich Deepfakes, produzieren oder teilen. Die Strafen werden noch härter, wenn die Technologie für Verbrechen wie Betrug oder Identitätsdiebstahl genutzt wird.

Dies ist ein Schritt in die richtige Richtung, aber bis weitere rechtliche Präzedenzfälle geschaffen sind, kann jeder in Sekundenschnelle ein Deepfake erstellen. Sollten also Sprach- und Video-Deepfakes illegal sein?

Prioritäten für das kommende Jahr

Angesichts der wachsenden Raffinesse von Betrugsbedrohungen ist es wenig überraschend, dass für 70 % der Befragten die strategische Überprüfung ihrer aktuellen Betrugslösungen oberste Priorität hat. Systeme, die über Jahre hinweg zuverlässig waren, geraten zunehmend an ihre Grenzen – und Unternehmen möchten mehr Betrugssignale in ihre Entscheidungsprozesse integrieren.

Diese Neubewertung ist eng verknüpft mit den folgenden Prioritäten: der Migration von Betrugslösungen in die Cloud (68 %) sowie der Investition in neue Betrugstools (ebenfalls 68 %).

In den nächsten drei bis fünf Jahren wird sich der Einfluss von GenAI auf das Betrugsgeschehen voraussichtlich weiter verstärken. Entsprechend entscheidend ist eine sorgfältige Auswahl der Investitionen in Technologien und Fähigkeiten zur Betrugsbekämpfung, um zusätzliche Verluste zu vermeiden.

Zukunftsorientierte Unternehmen setzen dabei zunehmend auf einheitliche, cloudbasierte Plattformen, statt verschiedene On-Premise-Einzellösungen zu kombinieren. Besonders wirkungsvoll ist die Verbindung von Betrugsprävention und Kreditrisikoprozessen: 69 % der Befragten planen, beide Bereiche künftig in eine integrierte Risikomanagementstrategie einzubetten.

Auch die Senkung der Untersuchungskosten zählt zu den zentralen Prioritäten. Automatisierung spielt dabei eine wichtige Rolle: Viele Betrugsteams bearbeiten Betrugswarnungen noch manuell, und 35 % berichten, dass solche Prüfungen eine Woche oder länger dauern. Mit den richtigen Betrugssignalen lässt sich ein deutlich größerer Anteil der Entscheidungen automatisieren – was Kosten reduziert und Betrugsexperten ermöglicht, komplexe Fälle schneller zu lösen.

Eine weitere wichtige Priorität ist die Investition in eine Orchestrierungsebene für Betrugstools (67 %). Ebenso viele Befragte sind überzeugt, dass die Orchestrierung mehrerer Betrugslösungen auf einer Plattform die Zukunft der Betrugsprävention darstellt. Die Vorteile liegen auf der Hand: Orchestrierung verbessert das Kundenerlebnis und senkt Kosten, da Betrugsprüfungen nur ausgelöst werden, wenn der individuelle Risikoscore dies erfordert.

Top 5 Betrugsprioritäten für das kommende Jahr

Basis: 979 leitende Entscheidungsträger im Bereich Betrug in EMEA & APAC
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

TEIL 2: Technologiegestützte Lösungen

Warum Machine Learning im Kampf gegen Betrug essenziell ist

Je mehr Daten in eine Bewertung einfließen – etwa Geräte- oder Verhaltensdaten –, desto präziser fallen die Ergebnisse aus.

Um diese großen Datenmengen effektiv zu nutzen, ist Machine Learning unverzichtbar. Nur ML verfügt über die analytische Leistungsfähigkeit, um Muster in umfangreichen Datensätzen zu erkennen. Das bestätigt auch unsere Studie: 67 % der ML-Nutzer berichten seit der Einführung von ML von einer messbaren Verbesserung der Betrugserkennungsgenauigkeit.

Ein weiterer entscheidender Vorteil von ML ist die Möglichkeit, Modelle kontinuierlich mit neuen Daten zu trainieren, sodass sie sich schnell an veränderte Betrugstaktiken anpassen. Regelbasierte Systeme hingegen stoßen hier an ihre Grenzen: Neue Regeln erhöhen die Komplexität und führen häufig zu mehr False Positives und zusätzlichen manuellen Prüfungen.

67 % der ML-Nutzer bestätigen, dass das kontinuierliche Neutrainieren und Aktualisieren ihrer Modelle ihnen hilft, mit der dynamischen Betrugsbedrohung Schritt zu halten. Der gleiche Anteil berichtet zudem von einem Rückgang der False-Positive-Rate seit Einführung von ML.

ML

70 %

stimmen zu, dass ML ihre Fähigkeit verbessert hat, Betrug zu erkennen, den ein rein regelbasiertes System übersehen hätte

Wie wirkt sich ML auf Unternehmen aus, die es eingeführt haben?

67 %

Unsere False Positive Rate ist seit der Implementierung von ML gesunken.

68 %

ML hat es uns ermöglicht, Sicherheitsbarrieren für gute Kunden durch passive Betrugsprüfungen zu reduzieren.

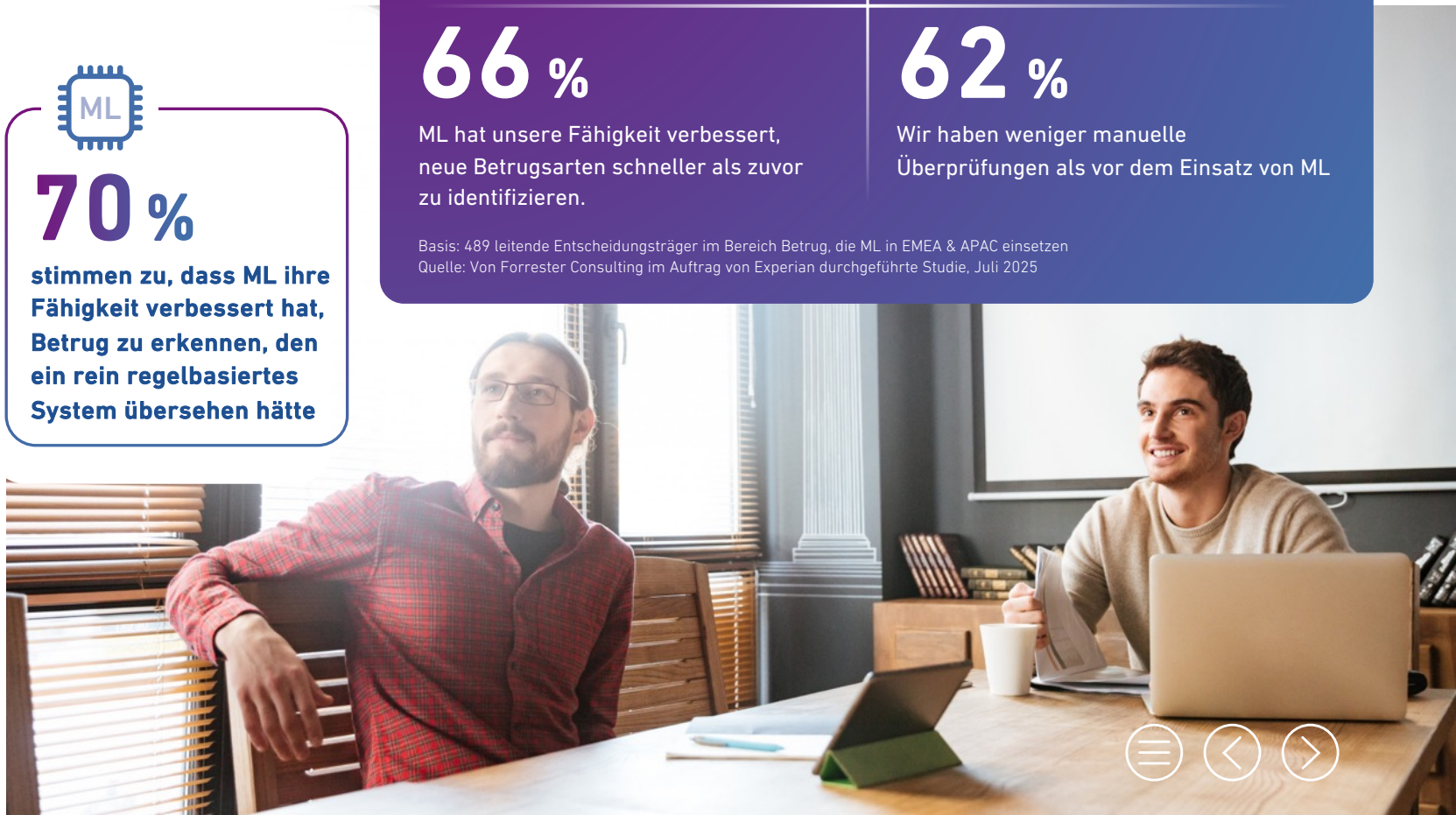
66 %

ML hat unsere Fähigkeit verbessert, neue Betrugsarten schneller als zuvor zu identifizieren.

62 %

Wir haben weniger manuelle Überprüfungen als vor dem Einsatz von ML

Basis: 489 leitende Entscheidungsträger im Bereich Betrug, die ML in EMEA & APAC einsetzen
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025



Was sind die wichtigsten Vorteile, die ML bietet?

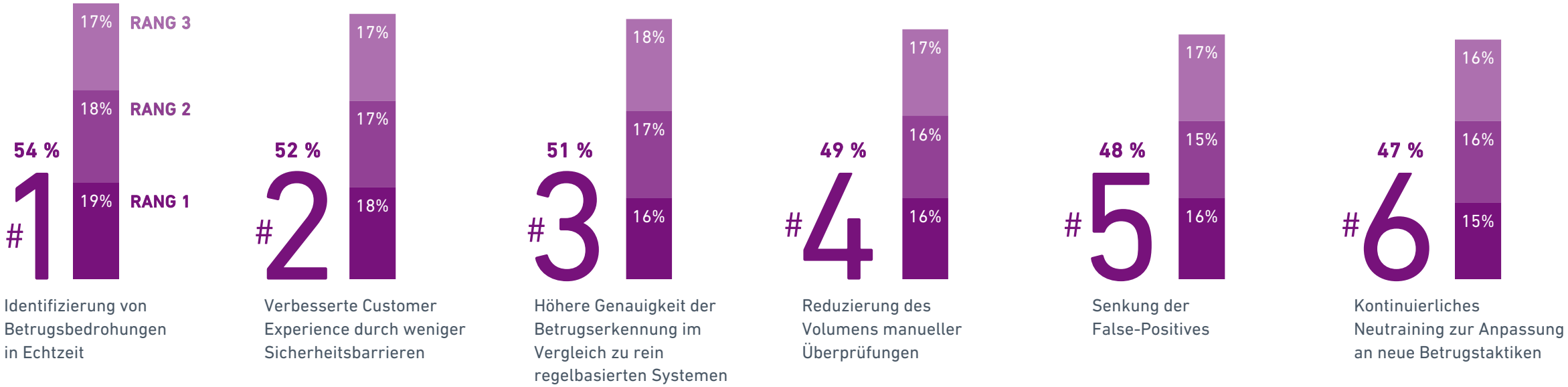
Unsere Untersuchung zeigt, dass der größte Vorteil der ML-Implementierung die Fähigkeit ist, Betrugsbedrohungen in Echtzeit zu erkennen (54 %). Derzeit können jedoch nur 33 % der Organisationen Betrug tatsächlich in Echtzeit identifizieren; 32 % benötigen dafür einen Tag oder weniger, und 35 % sogar eine Woche oder länger.

Der zweitgrößte Vorteil ist ein verbessertes Kundenerlebnis (52 %), das eng mit einer schnelleren Identifizierung von Betrug verknüpft ist. Kundenerlebnis bedeutet jedoch mehr als nur schnelle Entscheidungen: Ebenso wichtig ist die Reduzierung von Reibungsverlusten. Passive Betrugsprüfungen, die die Customer Journey nicht unterbrechen, spielen dabei eine zentrale Rolle.

Experian Experian bietet ein umfassendes Portfolio an aktiven und passiven Identitäts- und Betrugsprüfungen sowie eine preisgekrönte Orchestrierungsplattform, die Unternehmen dabei unterstützt, die optimale Balance zu finden.

In diesem kurzen Video sehen Sie, wie eine optimierte Customer-Onboarding-Journey aussehen kann.

Echtzeit-Erkennung bleibt der wichtigste Vorteil von Machine Learning



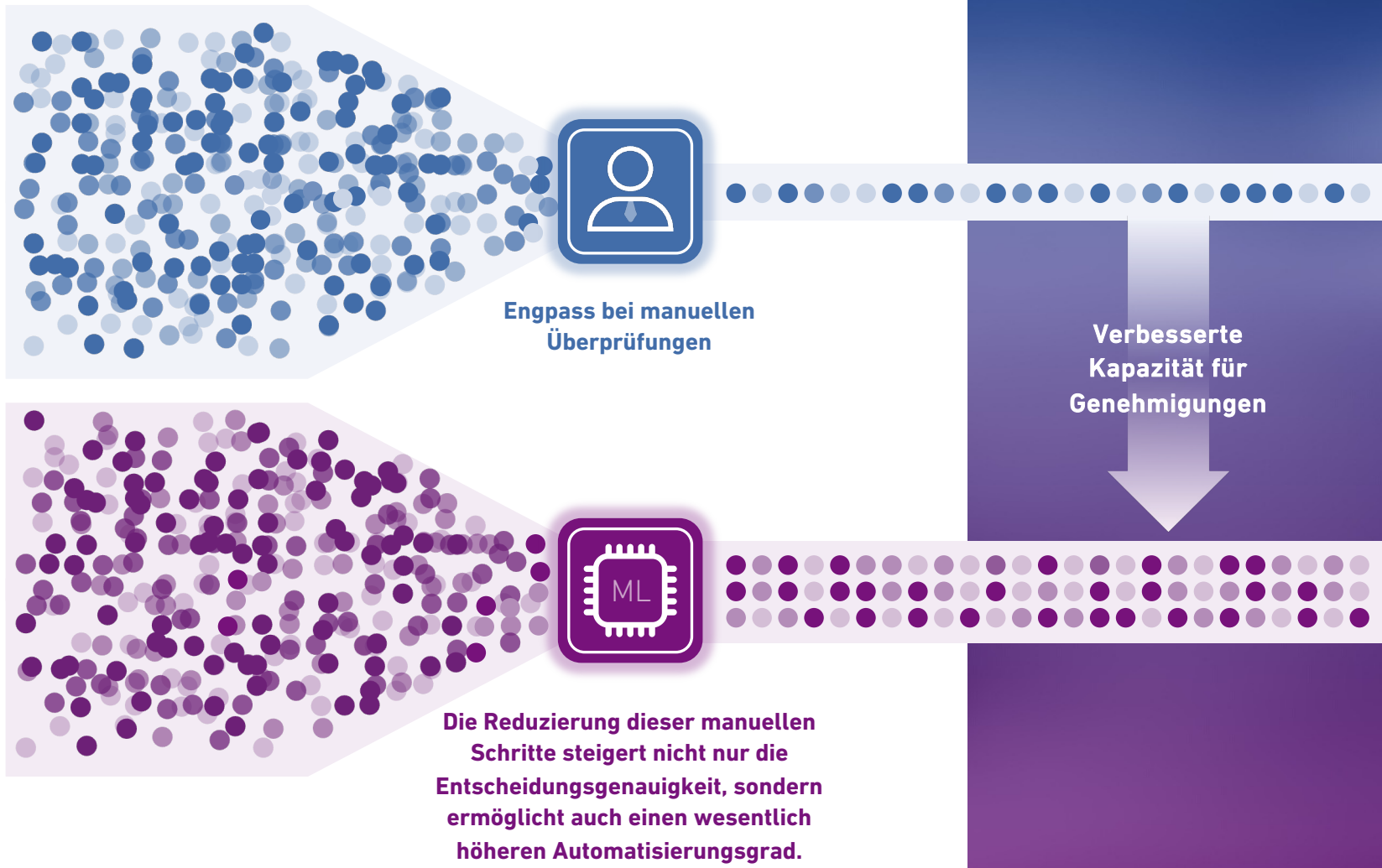
Basis: 489 leitende Entscheidungsträger im Bereich Betrug, die ML in EMEA & APAC einsetzen
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

ML kann Engpässe bei manuellen Überprüfungen deutlich reduzieren

ML kann Engpässe bei manuellen Überprüfungen deutlich reduzieren. Fast zwei Drittel (64 %) der Organisationen verlassen sich weiterhin auf manuelle Prüfungen zur Bearbeitung von Betrugswarnungen; im eCommerce liegt dieser Wert sogar bei 70 %. Die Folge: Gute Kunden erleben häufig langsame und frustrierende Antrags- oder Kaufprozesse – mit hohem Risiko von Abbrüchen.

ML liefert deutlich genauere Empfehlungen und schafft damit die Grundlage für mehr Automatisierung. 71 % der ML-Nutzer bestätigen, dass sie manuelle Prüffälle besser priorisieren können – was die Produktivität ihrer Betrugsanalysten spürbar erhöht.

Monatliche Anträge/Einkäufe mit und ohne ML



Warum wird ML nicht flächendeckend eingesetzt?

Ein Vergleich unserer aktuellen ML-Kreditrisikoforschung mit dieser Betrugsstudie zeigt ein klares Muster: Einige Entscheidungsträger im Kreditrisikoumfeld erkennen den Nutzen von ML noch nicht vollständig – und investieren daher nicht in entsprechende Lösungen.

Im Bereich der Betrugsprävention liegt der wichtigste Hemmschuh jedoch woanders: 73 % der Befragten geben an, dass es ihnen an ausreichend hochwertigen Trainingsdaten fehlt. Das zeigt, dass viele den Mehrwert von ML grundsätzlich verstehen – ihnen jedoch die Datenbasis zur Umsetzung fehlt.

Die Bedeutung ausreichender, qualitativ hochwertiger Trainingsdaten kann nicht hoch genug eingeschätzt werden. Präzise Betrugsprävention erfordert ausreichend vielfältige Datenquellen – und mit dem Aufkommen von ML ist ihr Stellenwert weiter gestiegen.

Trainingsdatensätze müssen groß und korrekt gelabelt sein, damit ML genaue Vorhersagen liefern kann. Vorgefertigte „Off-the-shelf"-Modelle können helfen, diese Herausforderung zu bewältigen, ebenso wie die Verwendung synthetischer Daten zur Ergänzung von Trainingsdatensätzen.

Regulatorische Bedenken bezüglich ML

Gesetzgeber weltweit arbeiten an Regelungen zur Nutzung von ML in der Betrugserkennung, um Transparenz und Fairness zu gewährleisten. Erklärbare ML-Modelle ermöglichen es abgelehnten Kunden, Entscheidungen nachzuvollziehen und anzufechten. Eine vollständige Auditierbarkeit stärkt zudem das Vertrauen von Fachanwendern in ML-basierte Entscheidungen.

ML-Modelle können vollständig erklärbar gestaltet werden und für jede Entscheidung eine nachvollziehbare Begründung liefern. Dennoch herrscht Unsicherheit darüber, welche Anforderungen Regulierungsbehörden genau stellen und wie diese umzusetzen sind. 71 % der Befragten wünschen sich mehr regulatorische Klarheit beim Einsatz von ML in Betrugspräventionssystemen.

67 % bestätigen, dass fehlende regulatorische Klarheit zu ML-Anwendungsfällen im Betrugsbereich die Einführung der Technologie bremst.

Interne Fähigkeit

Regularien

Interne Fähigkeit

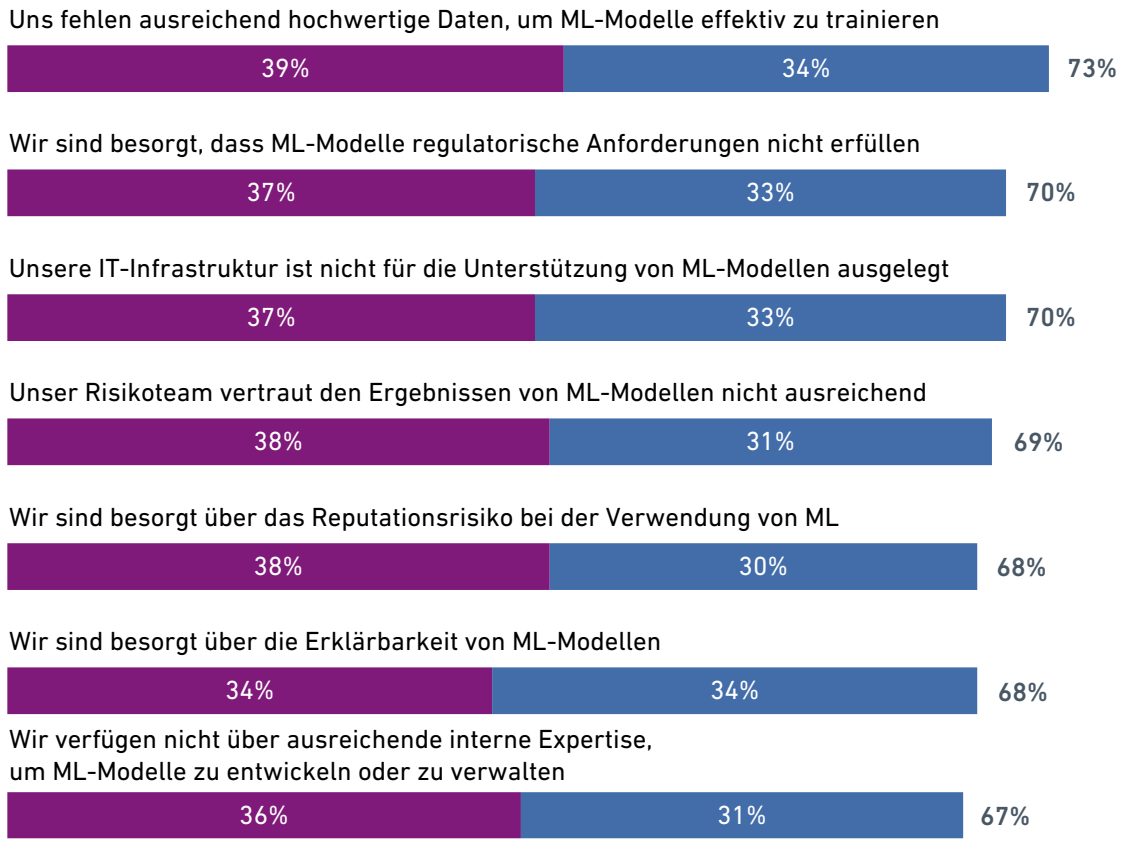
Vertrauen

Reputation

Regularien

Interne Fähigkeit

Hauptgründe für die Nicht-Einführung von ML



Basis: 490 leitende Entscheidungsträger im Bereich Betrug, die ML in EMEA & APAC einsetzen
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

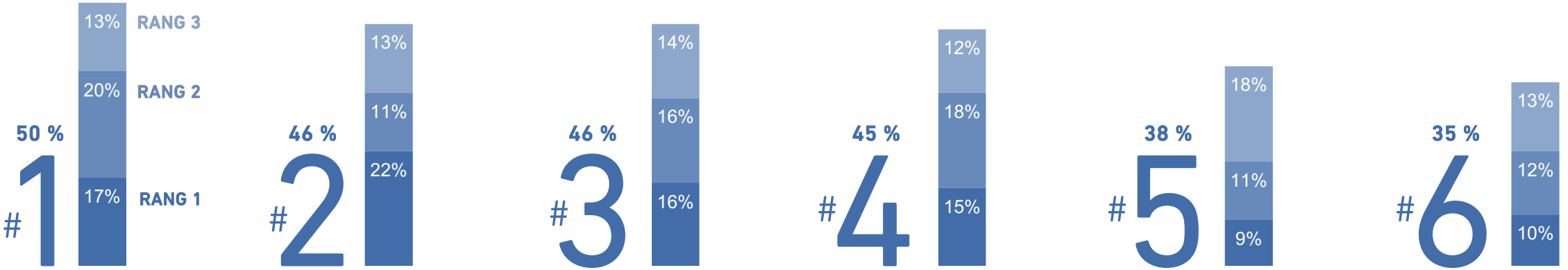
Welche Faktoren würden die Einführung von ML bei Nicht-Nutzern fördern?

Der wichtigste Treiber ist ein nachweisbarer ROI vergleichbarer Unternehmen. Wie bei vielen neuen Technologien verfolgen Organisationen gern die Strategie, „die Ersten zu sein, die Zweite sind" – also von den Erfahrungen anderer zu profitieren. Dieser Ansatz ist zwar risikoärmer, doch angesichts der aktuellen, erheblichen Betrugsbedrohung ist ein proaktiverer Einsatz moderner Technologien zur Betrugsprävention notwendg.

Viele Unternehmen haben ML bereits erfolgreich eingeführt und positive ROI-Ergebnisse erzielt. Bei einem Experian-Kunden lag der Zeitraum bis zum positiven ROI bei weniger als einem Monat – unmittelbar nach dem Go-Live wurde ein großer Syndikatsangriff identifiziert und verhindert.

Unternehmen, die den Mehrwert von ML bewerten möchten, können eine Offline-Proof-of-Value-(POV)-Analyse durchführen lassen. Dadurch lassen sich mögliche Vorteile anhand vorher definierten Kennzahlen nachvollziehen – ohne das ML-Modell direkt in bestehende Systeme integrieren zu müssen.

Ein nachweisbarer ROI und klarere regulatorische Vorgaben würden die Einführung von ML fördern



Basis: 490 leitende Entscheidungsträger im Bereich Betrug, die ML in EMEA & APAC einsetzen
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

GenAI-Assistenten und digitale Identitäts-Wallets

Eine Eine spannende Entwicklung im Betrugsmanagement sind GenAI-Assistenten, die direkt in Plattformen zur Betrugsprävention integriert werden. Diese Tools können wichtige Datenpunkte konsolidieren – etwa Regeln und deren Performance, Gründe für Betrugsentscheidungen sowie zeitliche Übereinstimmungen.

Sie können auch eine Fallrisikostufe bereitstellen, mit entsprechender Begründung und Anweisungen für „nächste Schritte“, um eine Untersuchung abzuschließen. Zusätzlich können sie manuelle Prozesse rationalisieren und sowohl die Effizienz als auch die Genauigkeit der Entscheidungsfindung verbessern.

Unsere Untersuchung zeigt, dass 80 % der Befragten den größten Vorteil eines GenAI-Assistenten darin sehen, Betrugspräventionsprozesse für weniger technische bzw. nicht programmierende Mitarbeitende deutlich zugänglicher zu machen.

Was könnte ein GenAI-Betrugsassistent für Ihr Unternehmen tun?

77 %

glauben, dass der größte Vorteil eines GenAI-Assistenten darin liegt, die Zeit für die Verwaltung von Betrugsfällen zu reduzieren.

72 %

stimmen zu, dass ein GenAI-Assistent, der hochgradig auf Betrugsdaten trainiert ist, ihnen helfen könnte, genauere Betrugsbewertungen vorzunehmen.

71 %

glauben, dass ein GenAI-gestützter Assistent die Zeit und den Aufwand für die Verwaltung neuer Betrugsfälle erheblich reduzieren könnte.

66 %

stimmen zu, dass ihre Organisation daran interessiert ist, diese Art von Technologie in ihre Betrugspräventions-Workflows zu integrieren.

Basis: 979 leitende Entscheidungsträger im Bereich Betrug in EMEA & APAC
Quelle: Von Forrester Consulting im Auftrag von Experian durchgeführte Studie, Juli 2025

Die Zukunft der digitalen Identitäten

Die EU hat kürzlich ihre Pläne für digitale Identitäts-Wallets konkretisiert, die gemäß eIDAS 2.0 im gesamten Block und international anerkannt werden sollen. In den nächsten zwei Jahren müssen alle Mitgliedsstaaten digitale Identitäts-Wallets anbieten, und Finanzdienstleister sowie Telco-Anbieter müssen diese akzeptieren.

Digitale ID-Initiativen werden auch in Singapur, Malaysia, Australien und vielen anderen Ländern eingeführt. Indien gilt mit seinem Aadhaar-Programm als Vorreiter - einem der weltweit am weitesten entwickelten digitalen Identitätssysteme mit über einer Milliarde registrierten Nutzenden.

74 % der Befragten sehen in digitalen Identitäts-Wallets eine strategische Chance zur Stärkung der Betrugsprävention. Ein ähnlicher Anteil (73 %) plant bereits aktiv, solche Lösungen in die eigene Customer Journey zu integrieren.

Digitale IDs haben das Potenzial, identitätsbezogenen Betrug deutlich zu reduzieren. Damit sich dieses Potenzial entfalten kann, sind jedoch umfassende staatliche und unternehmerische Aufklärungsprogramme notwendig, um Vertrauen und Akzeptanz zu stärken. Wie groß die Wirkung sein könnte, zeigen 70 % der Befragten, die bestätigen, dass digitale Identitäts-Wallets die Art und Weise, wie Kunden onboarded und authentifiziert werden, grundlegend verändern werden.

74 %

stimmen zu, dass die breite Einführung digitaler Identitäts-Wallets die Abhängigkeit von traditionellen KYC- und Dokumentenprüfungen deutlich reduzieren könnte.

Der Wandel zu Shared Fraud Intelligence

Kollektive Betrugsaufklärung wird zweifellos eine bedeutende Rolle in der Zukunft der Betrugsprävention spielen. **73 % der Befragten stimmen zu, dass der beste Weg, der Betrugsbedrohung zu begegnen, darin besteht, zusammenzuarbeiten und Betrug gemeinsam zu bekämpfen**.

Dieser Informationsaustausch muss jedoch von einem vertrauenswürdigen Dritten erleichtert werden – drei Viertel (75 %) glauben, dass der Aufbau von Vertrauen zwischen verschiedenen Mitgliedern eines Betrugskonsortiums der Schlüssel zu ihrem Erfolg ist.

Effektive Konsortien benötigen einen zentralen Management-Hub mit sicheren API-Verbindungen zu allen Mitgliedern. Dadurch können sensible Daten innerhalb des Netzwerks ausgetauscht werden – selbstverständlich unter Einhaltung aller regulatorischen Vorgaben. Jede Anfrage kann so gegen den gemeinsamen Intelligenzpool geprüft werden, ohne dass beteiligte Unternehmen Daten direkt miteinander teilen müssen.

74 %

stimmen zu, dass innerhalb der nächsten drei Jahre die Mehrheit der Unternehmen einer Shared-Fraud-Intelligence-Gruppe angehören wird.

Weitere Informationen zum Aufbau, zur Funktionsweise und zum Beitritt zu Konsortien finden Sie im Experian-Leitfaden:

DIE KRAFT GETEILTER INTELLIGENZ

Datentransferprozess in einem Konsortium

1

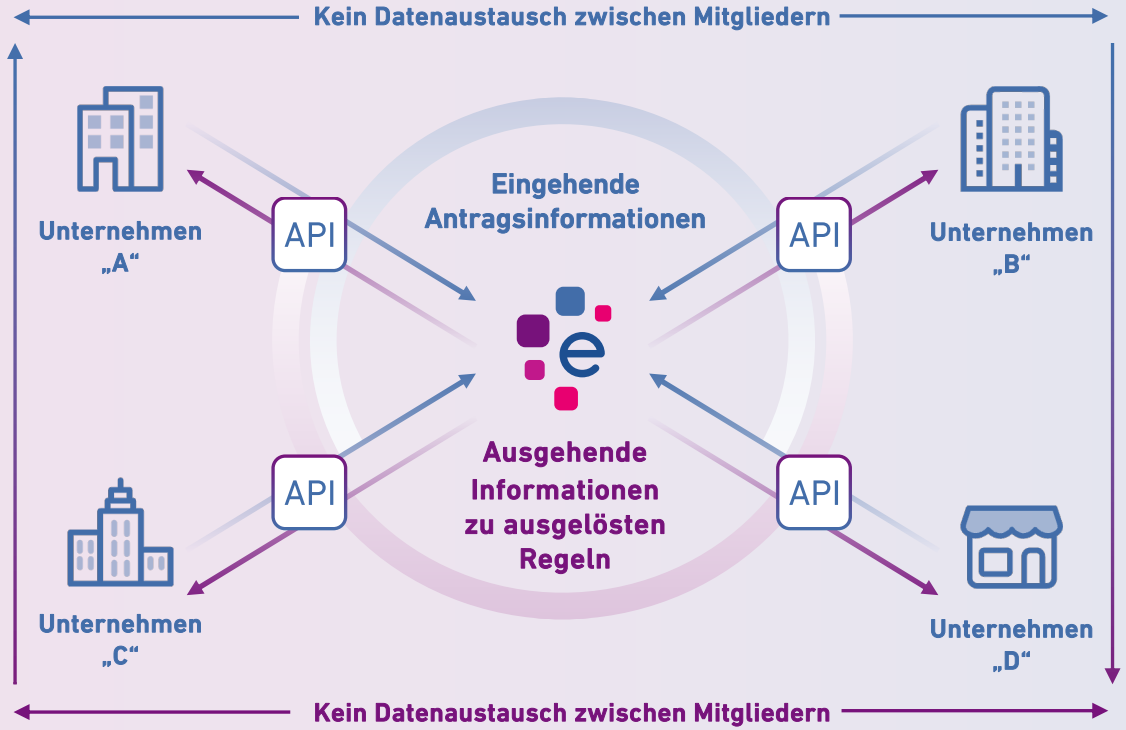
Jedes Unternehmen übermittelt seine Antrags- oder Transaktionsdaten über eine eigene, sichere API an den zentralen Hub.

2

Löst ein Antrag eine Warnung oder Regel aus, wird diese direkt an das jeweilige Unternehmen zurückgespielt.

3

Zwischen den Mitgliedern selbst findet keinerlei direkter Datenaustausch statt.



Wichtigste Erkenntnisse

GenAI und Deepfakes haben die Betrugslandschaft nachhaltig verändert. Mit zunehmender technologischer Ausgereiftheit dieser Tools werden zusätzliche Betrugssignale – etwa Geräte- und Verhaltensdaten – unverzichtbar, um einen weiteren Anstieg der Betrugsverluste zu verhindern.

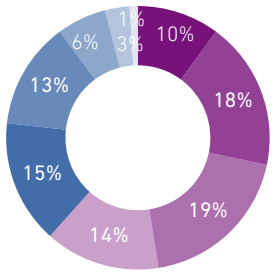
Eine strategische Überprüfung der bestehenden Betrugstools, um Fähigkeits- und Technologie-lücken zu identifizieren, bleibt die oberste Priorität für das kommende Jahr. Danach folgen die Migration von Betrugslösungen in die Cloud sowie Investitionen in neue, ML-gestützte Betrugstools.

Der wichtigste Vorteil von ML ist die Fähigkeit, Betrug in Echtzeit zu erkennen. Direkt dahinter folgt die Verbesserung des Kundenerlebnisses, da passive Betrugssignale reibungsärmere Onboarding- und Kaufprozesse ermöglichen.

Der Austausch kollektiver Betrugsinformationen über Konsortien wird in der zukünftigen Betrugsprävention eine zentrale Rolle spielen. Damit diese Zusammenarbeit funktioniert, braucht es jedoch einen vertrauenswürdigen, neutralen Dritten – sowohl zur Sicherstellung regulatorischer Konformität als auch zur Stärkung des gegenseitigen Vertrauens der Mitglieder.

Unternehmensdaten und Demografie der Befragten

UNTERNEHMENSUMSATZ



- über 5 Mrd. USD
- 1 Mrd. bis 5 Mrd. USD
- 500 Mio. bis 999 Mio. USD
- 400 Mio. bis 499 Mio. USD
- 300 Mio. bis 399 Mio. USD
- 200 Mio. bis 299 Mio. USD
- 100 Mio. bis 199 Mio. USD
- 50 Mio. bis 99 Mio. USD
- 50 Mio. bis 49 Mio. USD

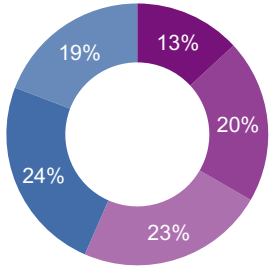
REGION

N=~109 pro Land

Dänemark, Spanien, Italien, Deutschland, Südafrika, Norwegen

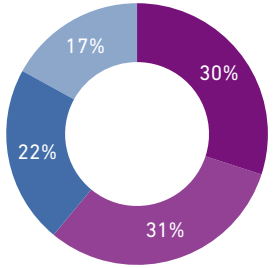
Neuseeland, Australien, Indien

HIERARCHIE-EBENE



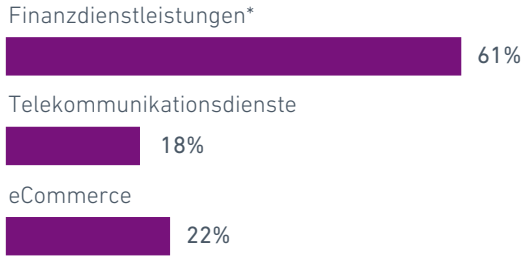
- C-Level-Führungskraft (z. B. CEO, CTO)
- Geschäftsführender Vizepräsident (EVP)
- Stellvetretender Geschäftsführer (SVP)
- Direktor
- Manager

UNTERNEHMENSGRÖSSE



- 500-999 Mitarbeiter
- 1,000-4,999 Mitarbeiter
- 5,000-19,999 Mitarbeiter
- 20,000 oder mehr Mitarbeiter

BRANCHE



*Bankwesen (38 %), Gewerbliche Finanzierung/Leasing (21 %), Kfz-Finanzierung (25 %), Verbraucherkredite (16 %)

DIREKTE VERANTWORTUNG FÜR DIE ENTSCHEIDUNGSFINDUNG

Glossar

API-BETRUGSANGRIFFE

Ausnutzen von Schwachstellen in APIs, um unbefugten Zugriff auf Daten zu erlangen, Denial-of-Service-Angriffe durchzuführen oder die API auf andere böswillige Weise zu manipulieren.

AUTHORISED PUSH PAYMENT (APP) BETRUG

Betrüger manipulieren Opfer durch Social Engineering, damit diese bereitwillig Zahlungen an sie leisten, indem sie beispielsweise vorgeben, von einem vertrauenswürdigen Finanzinstitut zu sein.

VERHALTENSBIOMETRIE

Identifizierung und Analyse von Datenpunkten, die mit der unterbewussten Art und Weise verbunden sind, wie ein bestimmter Benutzer mit seinem Gerät interagiert – ohne personenbezogene Daten zu sammeln. Dazu gehören Mausbewegungen, Tastenanschläge oder Touchscreen-Druck und viele hundert andere Verhaltensattribute.

VERHALTENSANALYSE

Identifizierung von Bot-Angriffen durch den Vergleich der Interaktion von Menschen mit Geräten gegenüber der Interaktion von Bots mit Geräten.

BOT/CREDENTIAL STUFFING

Automatisierte Betrugsangriffe, bei denen Listen gestohlener Zugangsdaten von einer Organisation verwendet werden, um unbefugten Zugriff auf ein Konto bei einer anderen Organisation zu erlangen.

DEVICE PROFILING/FINGERPRINTING

Analyse einer Reihe von Software- und Hardwareparametern, die mit einem bestimmten Gerät verbunden sind, um eine eindeutige Kennung bereitzustellen und das Risiko zu bewerten. Zu diesen Parametern gehören Betriebssystem, Netzwerk, Browser, Sprache, Zeitzone, Bildschirmverhältnis und viele mehr.

DEVICE INTELLIGENCE

Gerätedaten kombiniert mit Verhaltensdaten werden als Device Intelligence bezeichnet. Es liefert kontinuierliche und passive Betrugserkennungssignale.

DEEPFAKES

Video, Audio oder Bilder, die überzeugend verändert und manipuliert wurden, um jemanden so darzustellen, als würde er etwas tun oder sagen, was tatsächlich nicht getan oder gesagt wurde. Im Betrugskontext können sie verwendet werden, um KYC-Prüfungen mit einer gefälschten Persona zu täuschen.

FRAUD-AS-A-SERVICE (FAAS)

Betrugstools und -dienste, die meist im Darknet auf Pay-to-Use-Basis verkauft werden.

MONEY MULING

Eine Person, die hilft, kriminelle Gewinne zu waschen, indem sie Geld auf ihr Konto erhält und es dann im Auftrag eines Betrügers auf ein anderes Konto überweist. Diese Mittelsmänner werden oft über soziale Medien rekrutiert und sind sich möglicherweise nicht bewusst, dass Money Muling illegal ist.

PHYSISCHE BIOMETRIE

Einzigartige physische Merkmale, die zur Identifizierung einzelner Benutzer verwendet werden können. Zum Beispiel Lebenderkennung, die Gesichtserkennung verwendet.

SYNTHETISCHE IDENTITÄT

Eine Kombination aus echten und gefälschten personenbezogenen Daten wird verwendet, um eine schwer zu erkennende fabrizierte Identität zu erstellen.

SYNTHETISCHES UNTERNEHMEN

Wie eine synthetische Verbraucheridentität nutzen diese gefälschten Unternehmen eine Kombination aus echten und gefälschten Daten, um die Simulation eines legitimen Unternehmens zu erstellen.

DREIECKSBETRUG

Ein eCommerce-Betrug, bei dem ein Betrüger einen gefälschten Online-Shop erstellt, um Zahlungen von ahnungslosen Kunden zu sammeln, dann gestohlene Kreditkarteninformationen von einem Dritten verwendet, um dieselben Waren bei einem legitimen Einzelhändler zu kaufen und das Produkt an den ursprünglichen Kunden zu versenden. Der Kunde erhält seine Bestellung, der Betrüger behält das Geld ein, und der legitime Einzelhändler wird schließlich mit einer Rückbuchung vom Eigentümer der gestohlenen Karte belastet, was zu finanziellem Verlust und möglicher Schädigung seines Rufs führt.

Über Experian

Experian ist ein globales Daten- und Technologieunternehmen, das weltweit Chancen für Menschen und Unternehmen schafft.

Wir unterstützen dabei, Kreditvergabepraktiken zu modernisieren, Betrug aufzudecken und zu verhindern, Prozesse im Gesundheitswesen zu vereinfachen, digitale Marketinglösungen bereitzustellen und fundierte Einblicke in den Automobilmarkt zu gewinnen – basierend auf unserer einzigartigen Kombination aus Daten, Analytik und Software. Darüber hinaus helfen wir Millionen von Menschen, ihre finanziellen Ziele zu erreichen und sowohl Zeit als auch Geld zu sparen.

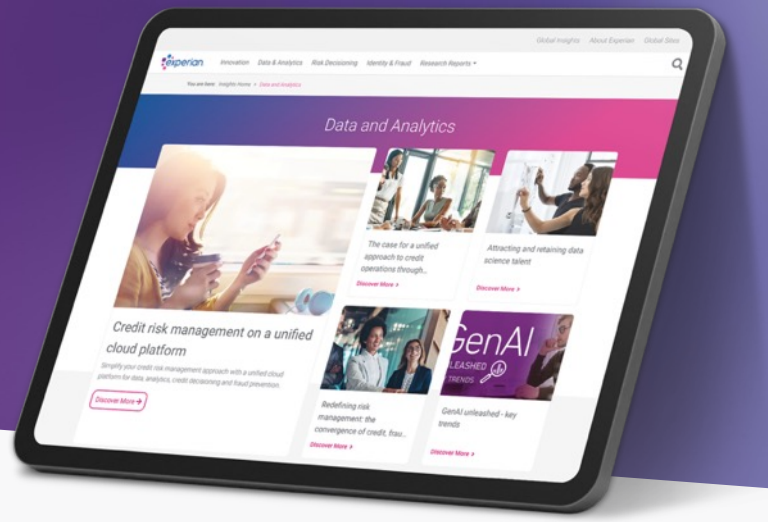
Wir sind in zahlreichen Märkten tätig – von Finanzdienstleistungen über Gesundheitswesen, Automobil und Agrarfinanzierung bis hin zu Versicherungen und vielen weiteren Branchen.

Wir investieren in talentierte Mitarbeitende und fortschrittliche Technologien, um das Potenzial von Daten zu entfalten und Innovationen voranzutreiben. Experian ist an der Londoner Börse (EXPN) gelistet und Teil des FTSE-100-Index. Weltweit beschäftigen wir rund 25.100 Mitarbeitende in 32 Ländern. Unser Hauptsitz befindet sich in Dublin, Irland.

Erfahren Sie mehr unter experianplc.com

Entdecken Sie mehr →

Kontaktieren Sie Ihren lokalen Experian-Berater oder besuchen Sie experianacademy.com



Registrierte Adresse: The Sir John Peace Building, Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ Telefon: 0844 481 9920 businessuk@experian.com experian.co.uk/business

© Experian 2025. Alle Rechte vorbehalten. Experian Ltd ist von der Financial Conduct Authority zugelassen und reguliert. Experian Ltd ist in England und Wales unter der Firmennummer 653331 registriert. Das Wort „EXPERIAN" und das grafische Symbol sind Marken von Experian und/oder seinen verbundenen Unternehmen und können in der EU, den USA und anderen Ländern eingetragen sein. Das grafische Symbol ist ein eingetragenes Gemeinschaftsgeschmacksmuster in der EU. Experian Public.