Betrugsbekämpfung und Identitätsprüfung: Sieben Trends für 2024

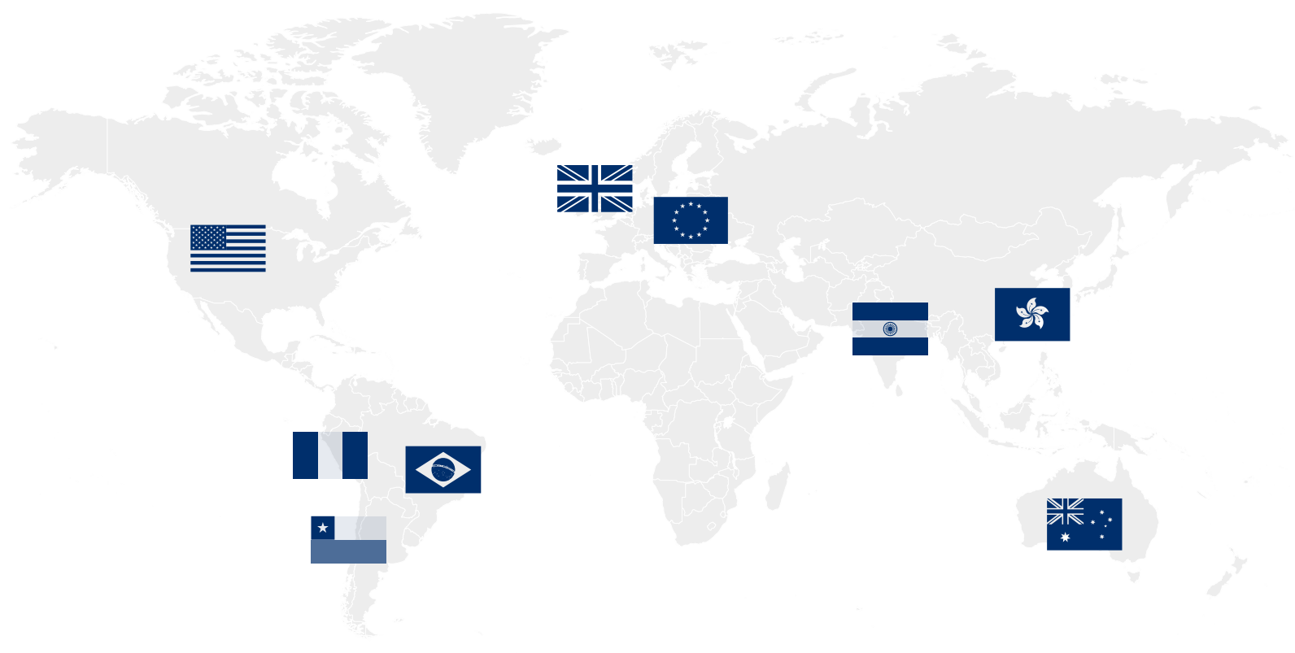
LexisNexis® RISK SOLUTIONS

Auf Experten im Bereich Betrugsbekämpfung und Identitätsprüfung warten zunehmende Herausforderungen: ein erhöhter regulatorischer Druck in vielen Teilen der Welt, das anhaltende Problem des synthetischen Identitätsbetrugs, die böswillige Nutzung künstlicher Intelligenz sowie immer besser vernetzte und grenzüberschreitende Betrugsangriffe.

Der Aufbau von Vertrauen und ein weiterhin positives Kundenerlebnis genießen hohe Priorität. Unternehmen, die 2024 eine neue Dimension der Betrugsprävention erreichen möchten, stehen diverse Möglichkeiten offen: ein verstärkter Einsatz von Verhaltensbiometrie zur Bekämpfung komplexer Betrugsfälle, die Nutzung der 360-Grad-Kundenansicht, die einen bemerkenswerten Mehrwert darstellt, oder ein kollaborativer Ansatz zur Betrugsbekämpfung, der enormes Potenzial bietet.

1 Zusätzlicher regulatorischer Druck wirkt sich voraussichtlich auf Risikomanagement-Kosten aus

Im kommenden Jahr werden Unternehmen noch mehr Ressourcen einsetzen, um die zunehmenden regulatorischen Anforderungen zu erfüllen.



USA: Haftung bei Verlusten nach Betrug sorgt für anhaltende Unsicherheit

Das Gesetz über elektronische Geldtransfers (Electronic Fund Transfer Act) könnte erweitert werden, um autorisierte betrügerische Überweisungen abzudecken. Vorausschauende Finanzinstitute ergreifen proaktive Maßnahmen, um Betrug zu erkennen und das Risiko zu minimieren.

82 %
Die meisten Führungskräfte von US-Finanzdienstleistern, die für Betrugsrisiken und Strategien zur Betrugsbekämpfung verantwortlich sind, gehen davon aus, dass Verbraucher erwarten, dass die Banken sie entschädigen, wenn ihre Konten erfolgreich für Betrugsmaschen missbraucht werden.[1]

66 %
der US-Verbraucher geben an, dass sie wahrscheinlich ihr Konto bei einem Institut schließen würden, das sie nicht für Verluste aufgrund von Überweisungsbetrug entschädigt.[2]

Vereinigtes Königreich: Neue Anforderungen für autorisierte Push-Zahlungen

Die britische Regulierungsbehörde für Zahlungssysteme hat ein neues obligatorisches Erstattungssystem für APP(Authorized Push Payment)-Betrug eingeführt, der Verbraucher im vergangenen Jahr schätzungsweise 630 Mio. USD gekostet hat.[3]

Die neuen Regeln verpflichten Banken und andere Zahlungsdienstleister dazu, Opfern von Betrug innerhalb weniger Tage die Kosten zu erstatten, wobei die Gesamtkosten zwischen der überweisenden und der empfangenden Institution aufgeteilt werden.

Obwohl die Zahlungen aufgrund von APP-Betrug im Jahr 2022 weniger als
0,1 %
des Gesamtvolumens schnellerer Zahlungen ausmachten, werden schnellere Zahlungen für
98 %
der APP-Betrugszahlungen genutzt.[4]

Die größten britischen Banken melden bis zu
439 USD
Verlust durch APP-Betrug pro überwiesenen 1,26 Mio. USD.[5]

Authorized Push Payments (APP) sind in den USA auch als „Authorized Transfer Scam" bekannt.

Europa: Vorschlag für eine neue Richtlinie über Zahlungsdienste und elektronische Gelddienste (PSD3)

PSD3 wird Anforderungen hervorbringen, die Verbraucherinteressen, Sicherheit und Vertrauen Vorrang einräumen. Die Vorschläge umfassen:

- Ausweitung der Erstattungsrechte von Betrugsopfern.
- Konsolidierung von E-Geld-Instituten und Zahlungsinstituten unter einem einheitlichen Regulierungssystem.
- Sicherstellung, dass die Verbraucher besser geschützt sind und ihre finanziellen Rechte besser kennen.

PSD2 fördert zwar den elektronischen Zahlungsverkehr und die Eindämmung von Betrugsfällen, aber die Kosten für die Umsetzung der Richtlinie – geschätzte
5,41 Mrd. USD –
und die erhöhte Rate fehlgeschlagener Transaktionen – geschätzte
36,2 Mrd. USD –
sind erheblich.[6]

Institute, die die Anforderungen von PSD2 nicht erfüllen, können mit Geldstrafen von bis zu
4 %
ihrer jährlichen Erträge belegt werden.

Lateinamerika: Neue Vorschriften für Gaming und Glücksspiel

Lateinamerikas regulierter Online-Glücksspielmarkt wird sich vervierfachen und bis 2027 einen Jahresumsatz von 6,75 Mrd. USD erreichen. Er ist sowohl für echte als auch für böswillige Akteure attraktiv.[8]

In Brasilien wurde 2023 ein neues Gesetz für Wetten und Online-Glücksspiele verabschiedet, das einen informellen Markt reguliert, der über
30 Mrd. USD
pro Jahr generiert.[9]

Die chilenische Regierung hat vor Kurzem einen Gesetzesentwurf eingebracht, der das Online-Glücksspiel wirksam legalisieren soll. Schätzungen zufolge könnte ein legalisierter Markt Einnahmen von mehr als
350 Mio. USD
pro Jahr generieren.[10]

In Peru wurden Vorschriften für Sportwetten und iGaming verabschiedet, die Mechanismen zum Schutz vor potenziellem Betrug schaffen.

Hongkong: Erhöhte E-Banking-Sicherheit

Die Hong Kong Monetary Authority hat zusätzliche Maßnahmen eingeführt, die die Sicherheit beim Online-Banking erhöhen und digitalen Betrug bekämpfen. Die Anforderungen sind für alle E-Banking-Aktivitäten obligatorisch und umfassen:

- Zusätzliche Kundenauthentifizierung.
- Überprüfung der Limits für grenzüberschreitende Überweisungen.
- Sitzungsmanagement-Kontrollen, die betrügerische Anmeldeversuche verhindern.
- Eine Pilotplattform für den Informationsaustausch zwischen Banken, die es ihnen ermöglicht, Risikoinformationen auszutauschen und schnellere Maßnahmen zur Risikominderung zu ergreifen.

Indien: Neue Ausrichtung in puncto Cybersicherheit, Risikokontrolle und IT-Governance

Banken und nicht der Bankenaufsicht unterliegende Unternehmen müssen die neuen 2023 eingeführten Vorschriften der indischen Zentralbank einhalten. Dazu gehört auch ein umfassender IT-Governance-Rahmen zur Minderung der Risiken von Cyberkriminalität

Von den 2021 fast 53.000 registrierten Fällen von Internetkriminalität handelte es sich in
60 %
der Fälle um Betrug.[11]

Australien: Regulierung für Anbieter digitaler Zahlungen

Neue von der australischen Regierung vorgeschlagene Regeln zielen darauf ab, die Anbieter digitaler Geldbörsen zu regulieren und der Zentralbank Australiens zu ermöglichen, diese Transaktionen auf die gleiche Weise zu überwachen wie Kreditkartennetzwerke.

Anstieg der Transaktionen mit mobilen Geldbörsen in Australien[12]

29,2 Mio.
2018

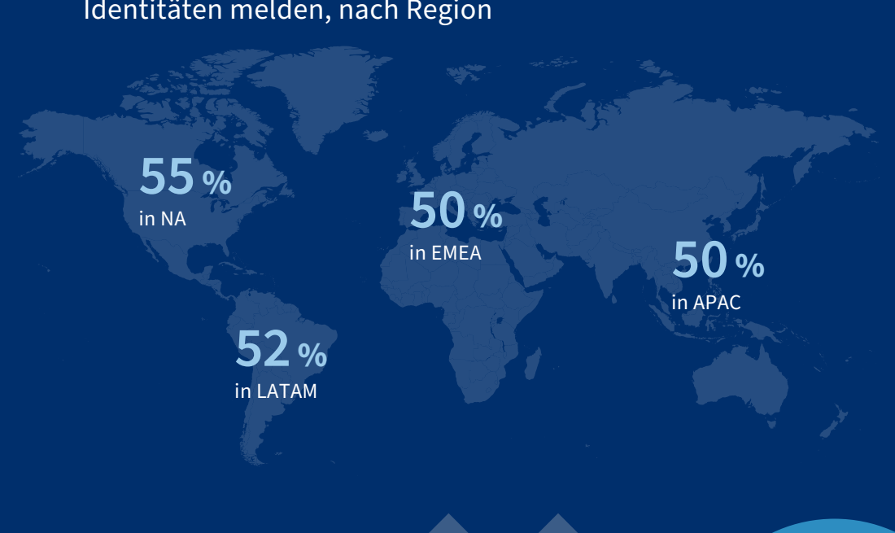
2,4 Mrd.
2022

2 Synthetische Identitäten: explosionsartiger Anstieg

Kriminelle nutzen die zunehmende Beliebtheit von digitalem Banking und E-Commerce, um neue betrügerische Konten mit synthetischen Identitäten zu eröffnen, die echte und gefälschte Informationen kombinieren. Die Bekämpfung von synthetischem Betrug stellt eine komplexe Herausforderung dar, die 2024 immer mehr an Bedeutung gewinnen wird.

48 % der Einzelhändler und **53 %** der Finanzdienstleister geben an, dass die Zunahme synthetischer Identitäten als größter mitbestimmender Faktor die Identitätsüberprüfung in Online-Kanälen besonders erschwert[13].

Prozentualer Anteil der Unternehmen, die einen Anstieg des Betrugs mit synthetischen Identitäten melden, nach Region



52 %
der Unternehmen weltweit berichten von einer Zunahme des synthetischen Identitätsbetrugs im Jahr 2023[14]

23 Mrd. USD
Erwartete Verluste aufgrund von synthetischem Identitätsbetrug in den USA bis 2030[15]

81.000 bis 98.000 USD[16]
beträgt der durchschnittliche Verlust durch einen unentdeckten synthetischen Identitätsbetrug

Prozentsatz der Betrugs- und Risikoverantwortlichen, die die Zunahme synthetischer Identitäten als die größte mitbestimmende Herausforderung für die Identitätsüberprüfung einschätzen ...

55 % bei der Kontoeröffnung

55 % beim Login

57 % bei Überweisungen / der Verteilung von Mitteln[17]

3 Zunehmende Nutzung künstlicher Intelligenz durch Kriminelle erfordert neue Taktiken zur Risikominderung

Die Nutzung von künstlicher Intelligenz (KI) mit böswilliger Absicht verändert die Betrugs- und Risikolandschaft. Die Bemühungen von Betrügern stellen sich immer häufiger als effektiv heraus und die Feststellung und der Nachweis von Identitäten stellen eine neue Herausforderung dar.

66 %
der Cybersecurity-Experten haben im Jahr 2022 Deepfake-Angriffe in ihren Unternehmen entdeckt[18]

90 %
der Online-Inhalte werden bis 2026 schätzungsweise synthetisch erzeugt[19]

38 %
der großen Unternehmen in EMEA und den USA waren 2023 von Deepfake-Betrug betroffen, was zu Verlusten von bis zu 480.000 USD führte[20]

4 Verstärkter Einsatz von Verhaltensdaten zur Bekämpfung komplexer Betrugsfälle

Verhaltensbiometrie wird für Unternehmen und Organisationen zu einem unverzichtbaren Instrument, um Vertrauen bei den Verbrauchern aufzubauen und immer raffinierteren Betrug zu verhindern. Vorausschauende Unternehmen verbessern ihre Strategie zur Betrugsprävention und schützen sich gegen ausgeklügelte Betrugsmaschen. Dabei setzen sie auf verhaltensbiometrische Daten.

Verhaltensdaten können an jedem Punkt der Customer Journey eingesetzt werden und dienen als Schutz vor den herausforderndsten Betrugsmaschen, die auf Verbraucher abzielen: APP-Betrug, Betrug per Fernzugriff und weitere komplexe Betrugsformen.

48 %
der Betrugsverantwortlichen zählten Betrugsangriffe auf Verbraucher zu ihren größten Sorgen im Jahr 2022.[21]

612 Mio. USD
Betrugsverluste durch autorisierte Push-Zahlungen (Authorised Push Payments, APP) in Großbritannien im Jahr 2022.[23]

35 %
der befragten US-Finanzdienstleister hatten bis September 2023 verhaltensbiometrische Lösungen implementiert.[22]

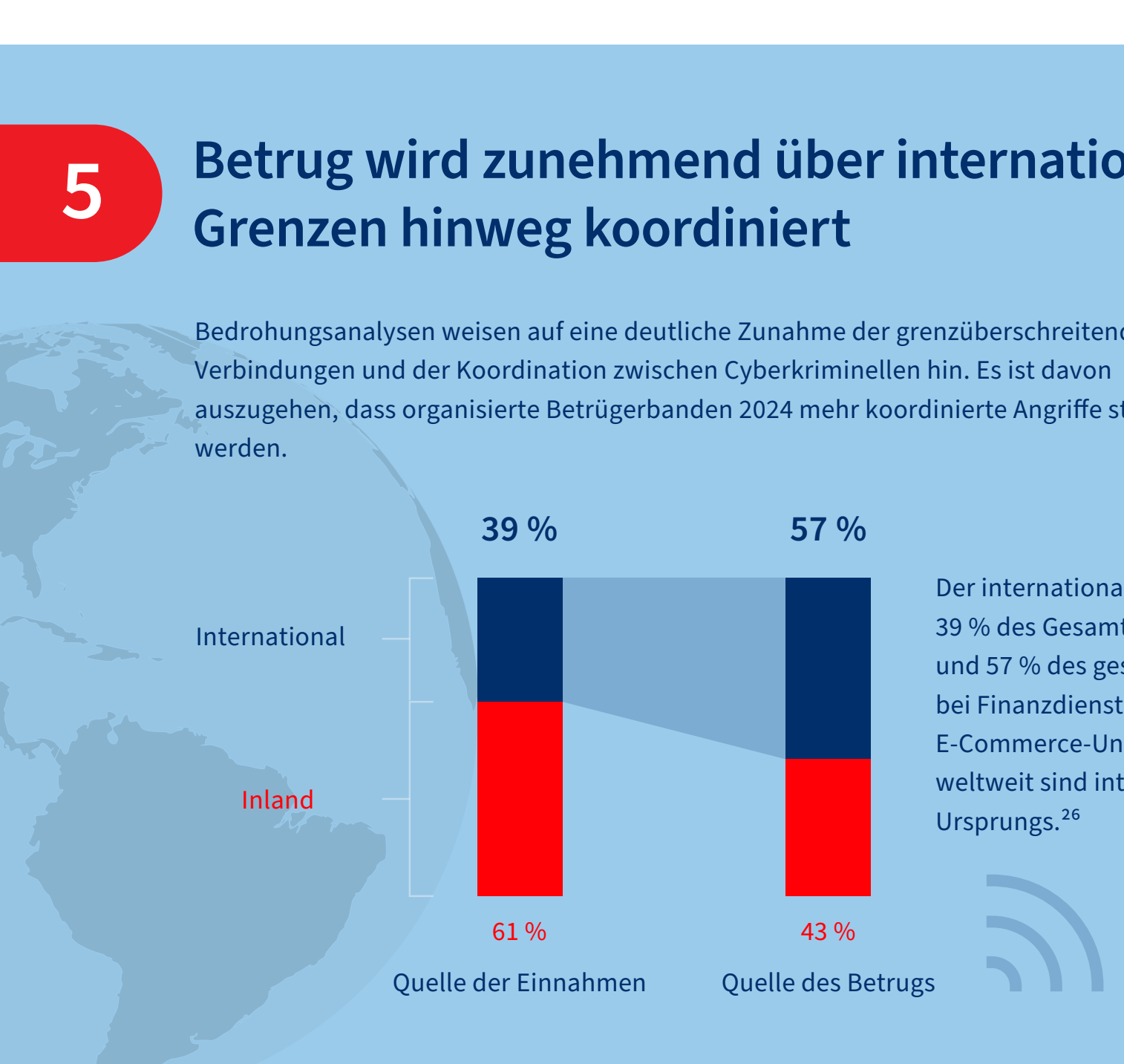
Weltweit nutzen
1/3
der Unternehmen verhaltensbiometrische Lösungen entlang der gesamten Customer Journey.[24]

Schlüsselfaktoren für die Einführung von verhaltensbiometrischen Lösungen[25]

- Digitalisierung beschleunigen
- Betrug bei der Neukonteneröffnung
- Kontoübernahme-Betrug
- Betrug mit autorisierten Push-Zahlungen (APP)
- Bedarf an starker Kundenauthentifizierung (SCA)
- „Know Your Customer" und Anti-Geldwäsche-Vorschriften
- Regulatorische Änderungen bei der Haftung
- Verbesserte Kundenerfahrung

5 Betrug wird zunehmend über internationale Grenzen hinweg koordiniert

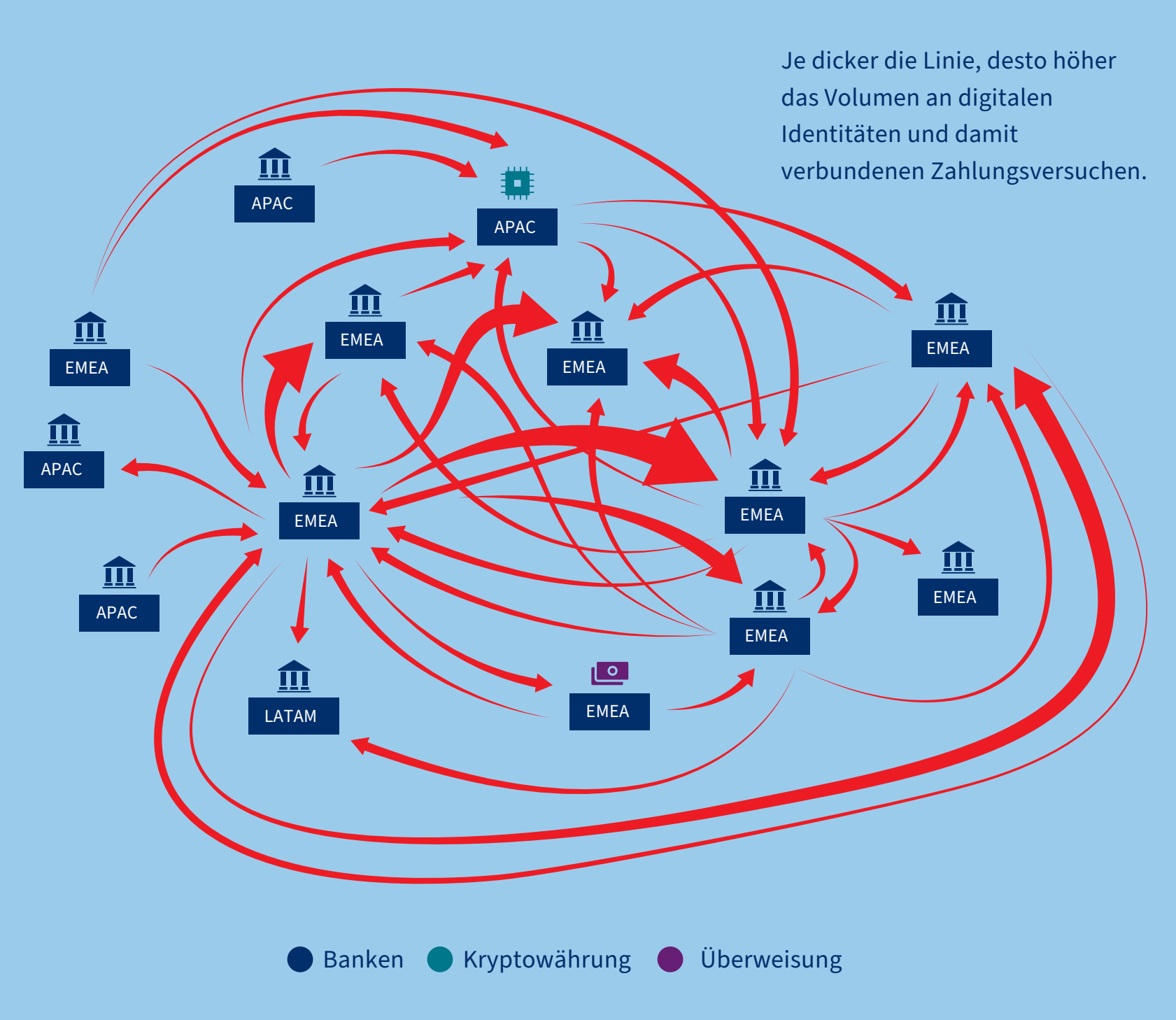
Bedrohungsanalysen weisen auf eine deutliche Zunahme der grenzüberschreitenden Verbindungen und der Koordination zwischen Cyberkriminellen hin. Es ist davon auszugehen, dass organisierte Betrügerbanden 2024 mehr koordinierte Angriffe starten werden.



Der internationale Umsatz macht 39 % des Gesamtumsatzes aus, und 57 % des gesamten Betrugs bei Finanzdienstleistern und E-Commerce-Unternehmen weltweit sind internationalen Ursprungs.[26]

Mule-Netzwerke, die durch digitale Identitäten verbunden sind, operieren über Regionen und Finanzinstitutionen hinweg, indem sie Zahlungsversuche bei einer Organisation unternehmen und dann zu anderen übergehen.[27]

Je dicker die Linie, desto höher das Volumen an digitalen Identitäten und damit verbundenen Zahlungsversuchen.



Prozentsatz der grenzüberschreitenden Betrugsanzeigen bei der Federal Trade Commission[28]

1 %
1992

11 %
2022

6 Die Einführung einer 360-Grad-Kundenansicht ist für eine bessere Risikobewertung unerlässlich

Ein besser integrierter und effektiverer Ansatz zur Betrugsbekämpfung beginnt mit dem Verständnis der Vielzahl von Kanälen und Interaktionen, die Kunden nutzen, um mit Unternehmen in Kontakt zu treten.

82 %
der Verbraucher, die mit ihrer Kreditkarte online einkaufen, sind auch aktive Nutzer des Online-Bankings derselben Bank, die die Kreditkarte ausgestellt hat. Digitale Identitätsdaten können also kanalübergreifend genutzt werden, um Vertrauen zu schaffen und komplexeren Betrug zu verhindern.[29]

3/4
der Befragten geben an, dass sich Betrug negativ auf ihre Marke und die Erfahrungen ihrer Kunden ausgewirkt hat.[30]

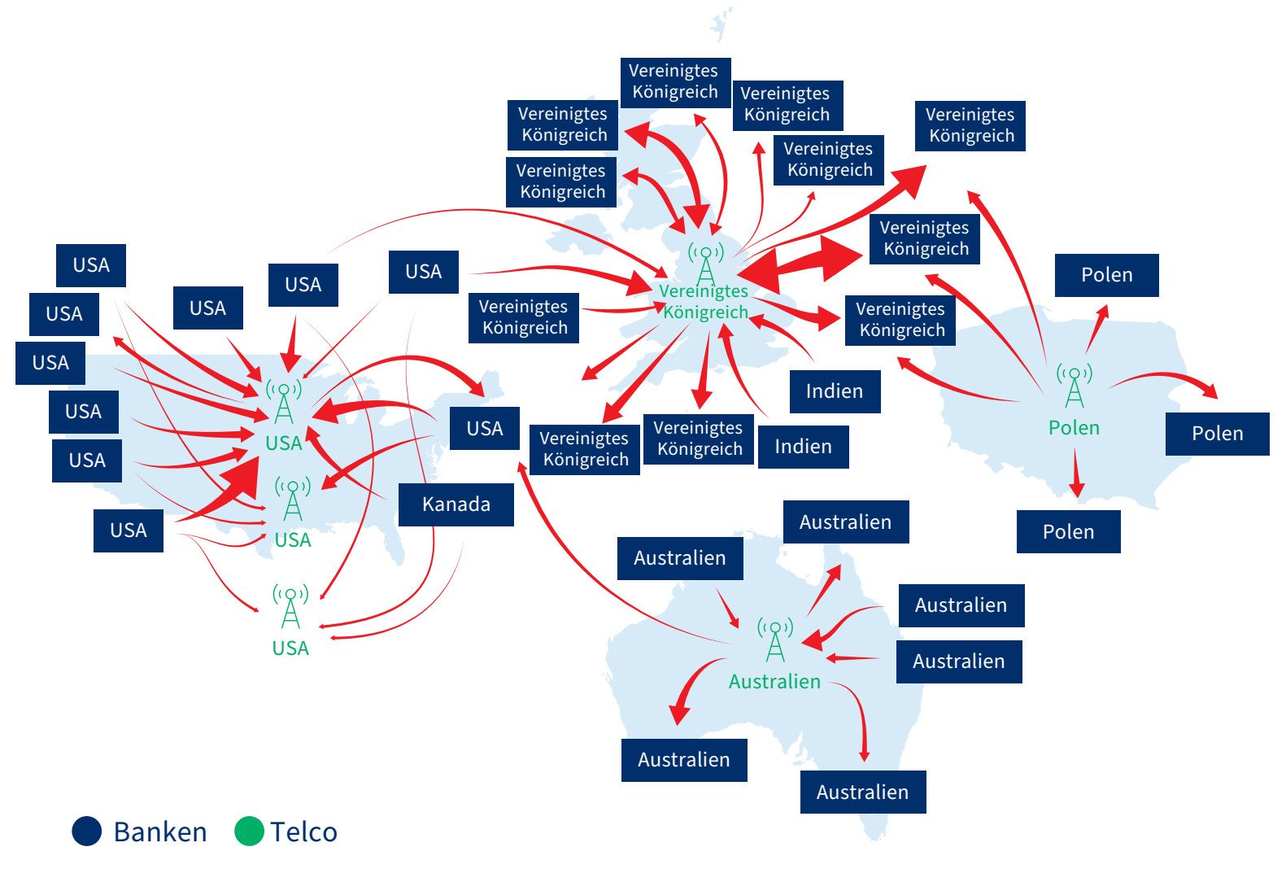
133 %
Anstieg der Anzahl der Banken, die im Jahr 2022 im Vergleich zu 2021 das LexisNexis® Digital Identity Network® sowohl im digitalen Banking als auch in den „3D Secure CNP"-Kanälen nutzen.[31]

60 %+
Verbesserung der Risikobewertung bei nachfolgenden Zahlungsvorgängen durch Erfassung kontextbezogener digitaler Informationen bei der Anmeldung.[32]

7 Kollaborativer Ansatz zur Betrugsbekämpfung

Initiativen zum Informationsaustausch, kollektive Intelligenz, Koordination von Maßnahmen und einheitliche Meldemechanismen: Das sind die Mittel, mit denen Cybersicherheitsunternehmen auch weiterhin arbeiten werden, um zunehmende Bedrohungen durch Betrug zu bekämpfen.

LexisNexis® Risk Solutions analysiert Jahr für Jahr etwa 80 Milliarden Transaktionen weltweit. Das LexisNexis® Digital Identity Network® sammelt Erkenntnisse von Tausenden von Unternehmen auf der ganzen Welt und baut so eine führende Datenbank für digitale Identitätsdaten auf, die mit jeder Transaktion leistungsfähiger wird.



Dieses Betrugsnetzwerk zeigt nur Verbindungen von mehr als zehn digitalen Identitäten an. Je dicker die Linie, desto höher das Angriffsvolumen.

Es werden regionale Betrugsnetzwerke veranschaulicht, die auf Banken und Mobilfunkbetreiber abzielen.

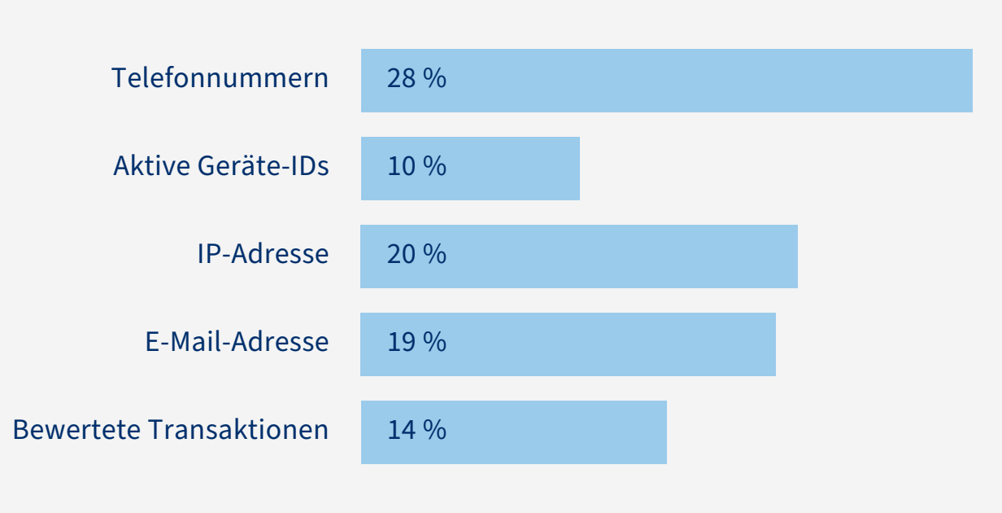
Die Angriffe auf den Finanzsektor werden zunehmend komplexer: Betrüger beginnen ihre Attacken oft damit, dass sie neue Mobilfunkverträge abschließen oder die Konten bestehender Mobilfunkkunden übernehmen. Im weiteren Verlauf benutzen sie diese für Übernahmeversuche oder für Neukontenbetrug.

Mindestens
2,4 Mio. USD
an Betrugswert gesperrt

Mindestens
10,3 Mio. USD
waren Betrug im gesamten Netzwerk ausgesetzt[33]

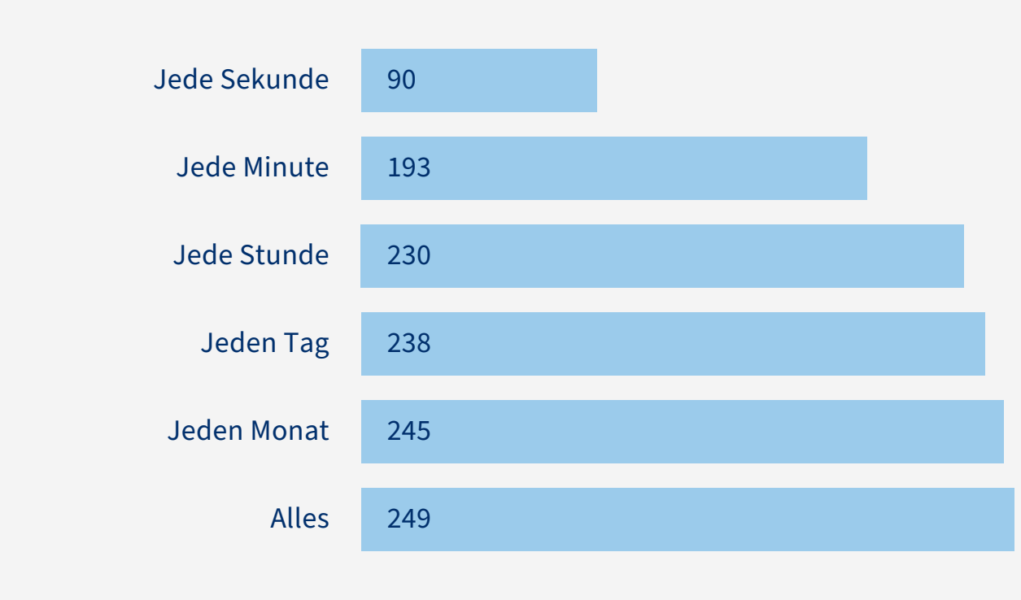
Die wichtigsten Datenelemente im LexisNexis® Digital Identity Network® vermehren sich schnell.

Wachstumsrate im Vorjahresvergleich pro Datenelement[34]



LexisNexis® Digital Identity Network®

Länder und Gebiete, die im Digital Identity Network® auftauchen[35]



LexisNexis® RISK SOLUTIONS

LexisNexis Risk Solutions

Mit seinen sieben Marken deckt LexisNexis® Risk Solutions verschiedene Branchen und Sektoren ab. Wir nutzen das Potenzial von Daten, fortschrittlichen Analyseplattformen und Technologielösungen, um Erkenntnisse zu liefern, die Unternehmen und Regierungsbehörden dabei helfen, Risiken zu reduzieren und Entscheidungen zu verbessern, die Menschen auf der ganzen Welt zugutekommen. Unsere Zentrale befindet sich in Atlanta, Georgia; zudem verfügen wir über Büros in verschiedenen Ländern weltweit. LexisNexis® Risk Solutions gehört zu RELX (LSE: REL/NYSE: RELX), einem globalen Anbieter informationsbasierter Analyse- und Entscheidungstools für Geschäftskunden. Weitere Informationen finden Sie unter LexisNexis Risk Solutions und RELX.

1 LexisNexis Risk Solutions True Cost of Fraud Study, 2023
2 LexisNexis Risk Solutions and Forrester, Authorized Transfer Scams: How financial institutions can transform an epidemic into an opportunity, 2023
3 UK Finance Annual Fraud Report, 2022
4 Payment Systems Regulator, APP scams performance report, 2023
5 Payment Systems Regulator, APP scams performance report, 2023
6 European Commission, A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)
European Banking Authority, Guidelines on the limited network exclusion under PSD2
The Fintech Times, Challenger Banks are Enabling the Most APP Fraud Reveals PSR Report, 2023
7 European Commission, A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)
8 Vixio, Latin America Online Outlook, 2023
9 Games Magazine Brazil, 2023
10 SBC News, 2023
11 Financial Times, India fights back against soaring digital fraud, 2023
12 Reuters, Australia unveils draft law to regulate digital payment providers, 2023
13 LexisNexis Risk Solutions True Cost of Fraud Study, 2023
14 LexisNexis Risk Solutions True Cost of Fraud Study, 2023
15 Deloitte Center for Financial Services, Using biometrics to fight back against rising synthetic identity fraud, 2023
16 Deloitte Center for Financial Services, Using biometrics to fight back against rising synthetic identity fraud, 2023
17 LexisNexis Risk Solutions True Cost of Fraud Study, 2023
18 World Economic Forum, How can we combat the worrying rise in the use of deepfakes in cybercrime?, 2023
19 World Economic Forum, How can we combat the worrying rise in the use of deepfakes in cybercrime?, 2023
20 World Economic Forum, How can we combat the worrying rise in the use of deepfakes in cybercrime?, 2023
21 Aite Novarica and LexisNexis Risk Solutions, Multifaceted Fraud Attacks, Behavioral Biometrics as a Defensive Tool, 2022
22 Aite Novarica and LexisNexis Risk Solutions, Multifaceted Fraud Attacks, Behavioral Biometrics as a Defensive Tool, 2022
23 UK Finance Annual Fraud Report, 2022
24 LexisNexis Risk Solutions True Cost of Fraud Study, 2023
25 Aite Novarica and LexisNexis Risk Solutions, Multifaceted Fraud Attacks, Behavioral Biometrics as a Defensive Tool, 2022
26 LexisNexis Risk Solutions True Cost of Fraud Study, 2023
27 LexisNexis® Risk Solutions Cybercrime Report, 2022
28 Federal Trade Commission Press Release, FTC Reports Outline Efforts to Combat Cross-Border Fraud and Ransomware Attack, 2023
29 LexisNexis® Risk Solutions Cybercrime Report, 2022
30 LexisNexis Risk Solutions True Cost of Fraud Study, 2023
31 LexisNexis® Risk Solutions Cybercrime Report, 2022
32 LexisNexis® Risk Solutions Cybercrime Report, 2022
33 LexisNexis® Risk Solutions Cybercrime Report, 2022
34 Data analysis from the LexisNexis® Digital Identity Network®
35 Data analysis from the LexisNexis® Digital Identity Network®