

Pressemeldung



Vier KI-Trends für 2026 von FICO

Analytics und KI gestalten Finanzbranche neu

- 1. GenAI-getriebene Betrugsmaschen nehmen massiv zu**
- 2. Fokussierte Sequenzmodelle revolutionieren die Transaktionsanalytik**
- 3. CIOs werden zu zentralen Veränderungstreibern in der Unternehmensführung**
- 4. Menschliche Aufsicht ist mehr denn je entscheidend für Cyber-Resilienz**

Berlin - 10. Februar 2026 – Im Jahr 2026 wird sich der Erfolg von KI im Finanzdienstleistungssektor laut [FICO](#) nicht an der Anzahl eingesetzter Modelle messen lassen, sondern an der Fähigkeit, Geschwindigkeit, Skalierung und Autonomie mit klaren Entscheidungsrahmen, Governance und menschlicher Verantwortung zu verbinden. Die Institute, denen dies gelingt, werden nicht nur effizienter arbeiten, sondern dauerhaft Vertrauen bei Kunden, Aufsichtsbehörden und Partnern aufbauen.

Mit Blick auf das Jahr 2026 hat FICO daher vier zentrale Trends identifiziert, die die Finanzbranche prägen werden:

1. GenAI-getriebene Betrugsmaschen nehmen massiv zu

Generative KI verändert das Betrugskosystem grundlegend. Kriminelle nutzen KI, um Stimmen zu klonen, Identitätsdokumente zu fälschen und personalisierte Betrugskampagnen in Sekundenschnelle zu skalieren. Laut einer globalen Umfrage von BCG waren 60 Prozent der Unternehmen bereits im vergangenen Jahr von KI-gestützten Angriffen betroffen, wobei Betrüger Angriffe nun in Sekunden statt Stunden ausführen.

Reaktive Betrugserkennung stößt dabei zunehmend an ihre Grenzen.

Insbesondere bei Identitätsprüfungen, nicht-monetären Transaktionen und autorisierten Push-Zahlungen bestehen weiterhin kritische Schwachstellen.

„Betrüger agieren heute mit Maschinengeschwindigkeit. Banken müssen deshalb von reaktiven Ansätzen zu einer proaktiven, ganzheitlichen Betrugsabwehr und Risikosteuerung übergehen, die jede Kundeninteraktion in Echtzeit bewertet und

frühzeitig eingreift. Der Erfolg im Kampf gegen Betrug erfordert zudem hochgradig personalisierte Kommunikationsstrategien, die Kunden sofort über ihre bevorzugten Kanäle (Textnachrichten, App-Benachrichtigungen oder E-Mail) erreichen, um verdächtige Aktivitäten zu verifizieren und einzugreifen, bevor finanzielle Verluste entstehen“, sagt TJ Horan, Vice President Fraud Product Management bei FICO.

2. Fokussierte Sequenzmodelle revolutionieren die Transaktionsanalytik

Fokussierte Sequenzmodelle (Focused Sequence Models, FSMs) markieren den größten Technologiesprung in der Transaktionsanalytik seit drei Jahrzehnten. Sie ermöglichen Entscheidungen mit extrem geringer Latenz und hohem Durchsatz, indem sie vollständige Transaktionshistorien in Echtzeit verarbeiten, anstatt sich auf isolierte Datenpunkte oder vereinfachte Durchschnittswerte zu stützen. So entstehen neue, deutlich präzisere Einblicke in Kundenverhalten und Risiken, die eine bislang unerreichte Personalisierung erlauben.

FSMs erfassen langfristige Transaktionssequenzen auf einzigartige Weise und decken kritische Zusammenhänge in Kundenhistorien auf, die traditionelle Analytics-Systeme meist übersehen.

„Die meisten Systeme analysieren Kundentransaktionen bislang isoliert oder verwenden starre, begrenzte Messgrößen von Transaktionshistorien – etwa Statistiken zu durchschnittlichen Ausgaben, Häufigkeitsmustern und geografischen Zuordnungen. Dadurch gehen entscheidende Verhaltensmuster verloren, die legitime Kunden von ausgefeilten Betrügern unterscheiden. Erst die Verarbeitung vollständiger Transaktionshistorien macht diese Unterschiede sichtbar“, erläutert Scott Zoldi, Chief Analytics Officer bei FICO.

3. CIOs werden zu zentralen Veränderungstreibern in der Unternehmensführung

Unternehmensweite KI-Initiativen haben einen Komplexitätsgrad erreicht, der klassische Abteilungsgrenzen überwindet. Agentische KI-Systeme treffen zunehmend autonome Entscheidungen im Kundenservice, bei Finanztransaktionen und in der strategischen Planung – und erfordern neue Governance-Regelwerke auf Unternehmensebene, die weit über die IT-Infrastruktur hinausgehen.

Laut der „2025 State of the CIO Survey“ von CIO.com priorisieren bereits 75 Prozent der CIOs KI höher als jede andere Technologieinvestition. Gleichzeitig zeigt die FICO Studie „State of Responsible AI in Financial Services: Unlocking Business Value at Scale“, dass 95 Prozent der befragten Finanzdienstleister eine Kluft zwischen KI-Initiativen und Erreichung von Geschäftszielen sehen. Damit wird klar: CIOs sind heute nicht mehr nur Technologieverantwortliche, sondern

Treiber des unternehmensweiten Wandels.

„CIOs haben sich von IT-Betreibern zu strategischen Führungspersönlichkeiten entwickelt. Mit agentischer KI im Einsatz prägen sie maßgeblich, wie Unternehmen Prozesse, Verantwortung und Wachstum neu organisieren“, Mike Trkay, Chief Information Office bei FICO.

4. Menschliche Aufsicht ist mehr denn je entscheidend für Cyber-Resilienz

KI hat das Schlachtfeld der Cybersicherheit grundlegend verändert. Angreifer verfügen nun über Werkzeuge für personalisiertes Phishing, die Erstellung von Deepfakes und die automatisierte Produktion von Malware – in bislang unerreichtem Umfang und mit enormer Geschwindigkeit. Gleichzeitig ist KI heute ein zentrales Element moderner Cyberabwehr. Doch rein automatisierte Schutzsysteme stoßen an ihre Grenzen. Modellmanipulationen, KI-Halluzinationen und komplexe Angriffsszenarien erfordern mehr denn je menschliches Urteilsvermögen, insbesondere wenn Entscheidungen gegenüber Aufsichtsbehörden und Stakeholdern erklärbar sein müssen.

Viele Unternehmen reagieren entschlossen: 41 Prozent der Unternehmen, die durch KI Produktivitätsgewinne erzielen, investieren diese laut EY US AI Pulse Survey 2025 gezielt in den Ausbau ihrer Cybersicherheitsfähigkeiten.

„Die effektivste Cyberabwehr entsteht nicht durch KI allein. Entscheidend ist die Kombination aus Maschinengeschwindigkeit und menschlicher Aufsicht, um Vertrauen, Transparenz und Resilienz sicherzustellen. Die Gewinner werden nicht diejenigen mit den leistungsstärksten Algorithmen sein, sondern diejenigen, die Maschinengeschwindigkeit mit menschlichem Urteilsvermögen verbinden“, sagt Ben Nelson, Chief Information Security Officer bei FICO.

-- ENDE --

Über FICO

FICO (NYSE: FICO) treibt Entscheidungen voran, die Menschen und Unternehmen auf der ganzen Welt zum Erfolg verhelfen. Das 1956 gegründete Unternehmen ist ein Pionier in der Anwendung von prädiktiver Analytik und Datenwissenschaft zur Verbesserung operativer Entscheidungen. FICO hält mehr als 200 US-amerikanische und internationale Patente auf Technologien, die die Rentabilität, Kundenzufriedenheit und das Wachstum von Unternehmen in den Bereichen Finanzdienstleistungen, Fertigung, Telekommunikation, Gesundheitswesen, Einzelhandel und vielen anderen Branchen steigern. Unternehmen in mehr als 80 Ländern vertrauen auf die bewährten Lösungen von FICO und schützen damit unter anderem 4 Milliarden Zahlungskarten vor Betrug, verhelfen Menschen zu Krediten und stellen sicher, dass Millionen von Flugzeugen und Mietwagen zum richtigen Zeitpunkt am richtigen Ort zur Verfügung stehen. Der FICO® Score, der von 90 % der führenden US-amerikanischen Kreditgeber verwendet wird, ist das Standardmaß für das Kreditrisiko von Verbrauchern in den USA. Darüber hinaus wurde er in über 40 weiteren Ländern verfügbar gemacht, um das Risikomanagement, den Zugang zu Krediten und die Transparenz zu verbessern.

Erfahren Sie mehr unter <https://www.fico.com/de/>.

FICO ist eine eingetragene Marke der Fair Isaac Corporation in den USA und anderen Ländern.

Besuchen Sie uns auch auf unserem [Blog](#).

Neuigkeiten und Informationen für Medienvertreter finden Sie unter <https://www.fico.com/en/newsroom>.

FICO Pressekontakt Deutschland:

Maisberger GmbH
Christine Wildgruber / Antonia Bodenschatz / Emma Deil-Frank
Claudius-Keller-Str. 3c
81669 München
Tel.: +49 89 419599 - 27 / -32 / -53
www.maisberger.com
fico@maisberger.com

Wenn Sie sich aus dem Verteiler austragen möchten, antworten Sie auf diese Mail bitte mit "Unsubscribe".