Flixcheck

# KI-Betrug erkennen, bevor er Schaden anrichtet

## Fraud Detection für Versicherer mit **Flixcheck Verify**

**Jetzt beraten lassen!**

# Warum Fraud Detection im Schadenmanagement jetzt Priorität hat

**Die Schadenabteilung ist seit jeher eine der sensibelsten Schnittstellen zwischen Versicherer und Kunde. Hier entscheidet sich, ob ein Leistungsversprechen eingelöst wird und ob dies wirtschaftlich tragfähig geschieht. Parallel dazu wächst der Druck auf Versicherer:**

- steigende Schadenaufwände und Kostendruck,
- erhöhte Erwartungen an Geschwindigkeit und Kundenerlebnis,
- zunehmende Professionalität von Betrugsversuchen – insbesondere durch den Einsatz von Künstlicher Intelligenz (KI)

Mit der Verbreitung generativer KI-Tools können heute realistische Schadensbilder mit wenigen Klicks erzeugt oder manipuliert werden. Für menschliche Prüfer ist es oft kaum möglich, solche Bilder von echten Aufnahmen zu unterscheiden, insbesondere bei hohem Fallaufkommen und unter Zeitdruck. Klassische Prüfmechanismen wie Plausibilitätschecks, Stichproben oder reine Metadaten-Analysen stoßen hier an ihre Grenzen.

**Für Versicherer entsteht dadurch ein neues Spannungsfeld:**
Einerseits sollen ehrliche Kundinnen und Kunden schnell, digital und möglichst friktionslos entschädigt werden. Andererseits müssen betrügerische Schäden frühzeitig erkannt und konsequent unterbunden werden, um Schadenquote und Prämienniveau stabil zu halten. Fraud Detection im Schadenmanagement ist damit kein „Nice-to-have“ mehr, sondern ein zentraler Bestandteil einer zukunftssicheren Schadenstrategie.

Wenn Sie nun vor der Frage stehen, wie Sie schnelle, digitale Schadenprozesse im Umgang mit Bildnachweisen und robuster Betrugserkennung verbinden können, liefert Ihnen dieses Whitepaper praxisnahe Orientierung und zeigt, wie Flixcheck Verify Sie dabei konkret unterstützen kann.

# 02

## Fraud Detection im Kontext der Versicherungsbranche

Fraud Detection ist im Schadenmanagement etabliert – verändert haben sich jedoch Tempo und Angriffsfläche: Digitale Eingangskanäle, hohe Fallzahlen und der Wunsch nach schneller Bearbeitung machen Bildnachweise zunehmend entscheidungsrelevant. Genau dadurch werden Fotos zum attraktiven Ziel, denn Manipulationen können Plausibilisierung, Priorisierung und sogar Dunkelverarbeitung gezielt beeinflussen.

# Typische Betrugs-szenarien im Schadenbereich mit Fokus auf Bildnachweisen

Im Zentrum stehen vor allem bild-getriebene Muster: bearbeitete Fotos realer Schäden (Retusche, Zuschnitt, Montage), um Ausmaß oder Kontext „passend“ zu machen, sowie Recycling/Dubletten, wieder-verwendete Bilder aus älteren Fällen oder externen Quellen. Häufig sind auch inszenierte Bildstrecken, die den gewünschten Hergang stützen, aber prüfkritische Perspektiven auslassen (z. B. nur Details ohne Übersicht oder Referenzen).

Hinzu kommt „technischer Nebel“ als Taktik: Screenshots statt Originalfotos, starke Kompression über Messenger oder Kanalwechsel (z. B. E-Mail statt Portal/App), wodurch Metadaten und forensische Spuren fehlen. Besonders verbreitet ist zudem Mischbetrug: Ein realer Schaden wird genutzt, um zusätz-liche Positionen zu begründen. Die Inkonsistenz zeigt sich oft erst im Zusammenspiel von Bildern, Angaben und Zeit-/Kontextlogik.

## Bisherige Methoden zur Betrugserkennung

Der bestehende Methodenmix bleibt unverzichtbar, hat aber in bildlast-igen Fällen typische Grenzen:

### Manuelle Prüfung

Ist flexibel und profitiert von Er-fahrung, skaliert jedoch schlecht und ist je nach Team und Zeitdruck uneinheitlich.

### Regelwerke/Scoring

Sind schnell und auditierbar, werden aber zunehmend umgangen und erzeugen bei Grenzfällen False Positives.

### Stichproben, Vier-Augen-Prinzip und SIU-Prozesse

Sind wirksam bei klarer Verdachts-lage, jedoch kapazitätsgebunden und häufig reaktiv.

### Historien- und Netzwerkchecks

helfen stark bei Serienmustern, liefern aber nicht immer eine belastbare Aussage „im Bild“.

### Klassische Bildforensik

(Metadaten, Dubletten, Artefakte) erkennt offensichtliche Mani-pulationen, stößt jedoch in der Praxis an Grenzen, wenn Metadaten fehlen, Bilder stark komprimiert sind oder Formate und Qualität stark variieren.

# Regulatorische Rahmenbedingungen und Reputationsrisiken

Fraud Detection ist regulatorisch und reputativ sensibel, weil sie direkt in Leistungsentscheidungen und Kundenerlebnis eingreift.

Verdachtsindizien und Prozessschritte müssen nachvollziehbar und auditfähig dokumentiert sein, während Bilddaten DSGVO-konform verarbeitet werden müssen (Zweckbindung, Zugriffskontrollen, Aufbewahrung).

Gleichzeitig ist der Umgang mit Verdachtsfällen eine Balance zwischen Wirksamkeit und Fairness: zu wenig Kontrolle erhöht das Risiko von Serienbetrug und steigenden Schadenquoten, zu harte oder intransparente Prüfungen führen zu Verzögerungen, Beschwerden und Vertrauensverlust.

Entsprechend brauchen moderne Ansätze nicht nur Treffer, sondern begründbare Hinweise für die Sachbearbeitung – konsistent, datenschutzkonform und sauber integrierbar in bestehende Schadenprozesse.

# 03

## Die neue Betrugs-dimension: KI-generierte Bilder und Deepfakes

Was sich aktuell verschiebt, ist weniger das „Ob“ von Bildmanipulation, sondern das Wie: Generative KI senkt die Einstiegshürde massiv und hebt gleichzeitig die Qualität. Damit entstehen Schadennachweise, die auf den ersten Blick plausibel wirken, sich schnell variieren lassen und in digitalen Prozessen deutlich schwerer zu entlarven sind besonders dann, wenn Bilder über verschiedene Kanäle und in heterogener Qualität eingehen.

# Was sind KI-generierte Bilder ?

z. B. Deepfakes oder generative Bildmodelle? KI-generierte Bilder entstehen durch Modelle, die Inhalte nicht nur bearbeiten, sondern neu erzeugen oder gezielt „umformen“. In der Praxis sind das vor allem drei Kategorien, die für Schadenprozesse relevant werden:

**Generative Bildmodelle**

*(z. B. für Text-zu-Bild)*

Es entstehen komplett neue Fotoszenen, die wie „echte“ Aufnahmen aussehen können – inklusive Licht, Perspektive und Details.

**Bildbearbeitung mit KI**

*(Inpainting/Outpainting, „Generative Fill“)*

Reale Fotos werden punktgenau verändert, ohne dass klassische Bearbeitungsspuren deutlich sichtbar sind (z. B. Kratzer ergänzen, Brandspuren verstärken, Wasserflecken plausibilisieren).

**Deepfakes**

*(Bild/Video)*

Inhalte werden so verändert, dass Personen, Umgebungen oder Situationen real wirken – für den Schadenbereich eher indirekt relevant, aber zunehmend als Teil „stimmiger“ Fallnarrative (z. B. Videoausschnitte, vermeintliche Belege).

# Warum klassische Prüfmechanismen hier an ihre Grenzen stoßen

Viele etablierte Kontrollen setzen implizit darauf, dass Manipulation entweder handwerkliche Spuren hinterlässt oder dass Kontextdaten (Metadaten, Originaldateien, konsistente Serienlogik) verlässlich verfügbar sind. Genau das wird durch generative KI schwieriger:

### Weniger verwertbare Metadaten:

In realen Eingangskanälen fehlen EXIF-Daten häufig ohnehin (Screenshots, Messenger, Kompression). KI-Manipulation braucht sie nicht und passt damit „perfekt“ in metadatenarme Prozesse.

### Hohe visuelle Plausibilität bei geringer Varianz:

Moderne KI kann Licht, Texturen und Perspektiven so konsistent erzeugen, dass selbst geübte Prüfer im Tagesgeschäft nur schwer belastbare Indizien finden – besonders unter Zeitdruck.

### Regelbasiertes Scoring wird leichter umgangen:

Wenn Betrüger Varianten in Minuten erzeugen können, passen sie Motive, Bildausschnitte und Qualität so an, dass einfache Heuristiken (zu „perfekt“, zu „unscharf“, falsches Format) nicht mehr greifen.

### Manuelle Prüfung skaliert nicht:

Wenn Verdachtsfälle steigen, steigen auch Rückfragen und Eskalationen – die Folge sind längere Durchlaufzeiten und ein höheres Risiko von Fehlentscheidungen (False Positives wie False Negatives).

Klassische Prüfmechanismen bleiben wichtig, aber sie sind ohne zusätzliche, spezialisierte Signale im Bild zunehmend nicht mehr trennscharf genug.

# Konkrete Bedrohungs-szenarien für Versicherer

### Manipulierte Schadensfotos

Reale Fotos werden mit KI so verändert, dass der Schaden plausibel „aufgewertet“ wird. Typisch sind Ergänzungen oder Verstärkungen (z. B. Kratzer/Dellen, Bruchkanten, Feuchtigkeitsspuren), das Entfernen von Kontext (Vorschäden, Umgebung) oder das „Repa-rieren“ von Widersprüchen im Bild (z. B. störende Details, die nicht zum Hergang passen). Das Ergebnis wirkt wie ein normales Handyfoto.

### Vollständig synthetische Schäden

Hier wird nicht mehr ein Bild manipuliert, sondern der gesamte Nachweis erzeugt: plausible Fotos eines beschädigten Gegenstands oder einer Situation, die so aussehen, als wären sie vor Ort aufgenommen worden. In digitalen Prozessen, vor allem dort, wo schnelle Regulierung gewünscht ist und weitere Nachweise minimal gehalten werden steigt dadurch das Risiko, dass Fälle überhaupt erst in den Prozess „hineinrutschen“, bevor sie auffallen.

### Serienbetrug mit skalierbaren KI-Inhalten

Der größte Hebel liegt in der Skalierung: Ein einmal funktionierendes Muster kann als Vorlage dienen und in kurzer Zeit in vielen Varianten ausgespielt werden (andere Perspektive, anderer Hintergrund, andere Schadenintensität). Kombiniert mit kanalübergreifender Einreichung (E-Mail/Portal/App/Checks) entsteht eine neue Art von „Betrugsautomation“, bei der Masse und Variation die Erkennung erschweren.

03 | Die neue Betrugsdimension

# Auswirkungen auf Schaden-quote, Bearbeitungszeiten und Kundenvertrauen

Operativ führt das zu mehr „Leakage“-Risiko (unberechtigte Zahlungen), mehr Prüfaufwand und einer Verschiebung der Arbeit in Richtung Triage und Eskalation. Gleichzeitig steigt das Spannungsfeld im Kundenerlebnis: Wenn Sie Kontrollen verschärfen, drohen mehr Rückfragen und längere Laufzeiten für legitime Fälle; wenn Sie Prozesse schlank halten, wächst das Risiko systematischer Ausnutzung

**Reputativ wirkt beides**

Sichtbare Betrugswellen schaden Vertrauen in Prämienlogik und Leistungsfähigkeit – zu harte oder uneinheitliche Prüfungen schaden Vertrauen in Fairness und Service.

# 04

## Herausforderungen für Versicherer in der Praxis

Die beschriebenen Betrugsmuster treffen in der Realität auf Schadenorganisationen, die unter einem konstanten Spannungsfeld arbeiten: schnell regulieren, Kundenerlebnis sichern, Kosten im Griff behalten und gleichzeitig Missbrauch erkennen. Gerade bei bildbasierten Nachweisen entsteht dadurch eine Lücke zwischen Anspruch und Alltag, die Betrüger gezielt ausnutzen.

# Operative Herausforderungen in Schadenabteilungen

### Zeitdruck und hohe Fallzahlen

Schadenprozesse sind heute stark getaktet: SLAs, digitale Erwartungshaltung und die zunehmende Automatisierung von Standardfällen erhöhen den Druck, schnell zu entscheiden.

Gleichzeitig steigt die Zahl der Fälle, in denen Bilder entscheidungsrelevant sind, als primärer Nachweis oder als Trigger für Priorisierung und Dunkelverarbeitung.

In dieser Situation wird Betrugserkennung häufig „nebenbei“ geleistet: als Zusatzaufgabe zur eigentlichen Fallbearbeitung. Genau das macht sie anfällig, denn KI-generierte oder manipulierte Bilder sind darauf ausgelegt, im schnellen Sichtcheck nicht aufzufallen.

### Manuelle Bildprüfung als Kostentreiber

Manuelle Bildprüfung ist teuer, weil sie Expertise bindet und nicht linear skaliert. Wenn Verdachtsfälle zunehmen, steigen Rückfragen, Eskalationen und SIU-Tickets, oft ohne klare Trennschärfe.

Das Ergebnis sind höhere Bearbeitungskosten pro Fall und längere Durchlaufzeiten, auch für legitime Kundinnen und Kunden. Gleichzeitig bleibt ein Restrisiko:

Wenn Teams wegen Überlastung „durchwinken“, entsteht Leakage; wenn sie zu streng prüfen, entstehen False Positives und ein spürbarer Disput im Kundenerlebnis.

04 | Herausforderungen für Versicherer

# Technische Herausforderungen

### Heterogene Input-Kanäle

Bilder kommen selten über einen einzigen Kanal. In der Praxis laufen Nachweise über E-Mail, Kundenportale, Apps, Messenger-Weiterleitungen oder strukturierte Prozesse wie digitale Formulare/Checks ein. Jeder Kanal bringt andere Qualitäts- und Kontextbedingungen mit: mal mit Originaldatei, mal als Screenshot, mal als komprimierter Upload. Für Fraud Detection bedeutet das: Die Prüfbasis ist nicht standardisiert und Signale, die in einem Kanal verfügbar wären, fehlen im nächsten.

### Unterschiedliche Bildqualität, Metadaten und Formate

Selbst bei ähnlichen Fällen unterscheiden sich Bilder stark: Auflösung, Kompression, Ausschnitt, Dateiformate und Bearbeitungshistorie variieren. Metadaten (EXIF) fehlen häufig vollständig oder sind nicht verlässlich, weil sie durch Upload-Strecken entfernt werden. Genau diese Realität begünstigt KI-Manipulation: Moderne generative Verfahren sind nicht auf Metadaten angewiesen und liefern Ergebnisse, die visuell plausibel wirken, auch bei niedriger Qualität. Klassische forensische Indikatoren werden dadurch weniger trennscharf, wenn sie isoliert betrachtet werden.

# Organisatorische und rechtliche Herausforderungen

**Dokumentationspflichten**

Verdachtsentscheidungen müssen begründet werden können, intern (Qualitätssicherung, SIU-Prozesse) und extern (Beschwerden, Rechtsstreit, Aufsicht). In der Praxis bedeutet das: Wer einen Fall markiert oder verzögert, braucht nachvollziehbare Indizien und eine saubere Dokumentationslogik, die in bestehende Workflows passt.

**Nachvollziehbarkeit und Auditfähigkeit von Entscheidungen**

Je stärker Fraud Detection automatisiert wird, desto wichtiger wird Auditfähigkeit: Welche Signale lagen vor? Welche Schwelle wurde genutzt? Welche Folgeprozesse wurden ausgelöst? Ohne nachvollziehbare Entscheidungsgrundlage entsteht ein Risiko, nicht nur rechtlich, sondern auch für die Akzeptanz in den Teams. Moderne Lösungen müssen daher Ergebnisse liefern, die operativ verwertbar sind: als konsistenter Hinweis, als Score oder als klarer Trigger für Triage und Eskalation.

**Datenschutz & DSGVO**

Bilddaten sind personenbezogen oder können es sein – insbesondere, wenn Personen, Kennzeichen, Adressen oder Dokumente enthalten sind. Damit gelten klare Anforderungen an Zweckbindung, Zugriff, Aufbewahrung und Verarbeitung. Für Versicherer heißt das: Fraud Detection muss DSGVO-konform gestaltet sein, ohne dass sie dadurch praktisch unbrauchbar wird. Entscheidend ist, dass Lösungen datenschutzfreundlich integriert werden können – mit klaren Rollen- und Rechtekonzepten und ohne unnötige Datenweitergabe oder manuelle Umwege.

# 05

## Die Rolle von KI in der modernen Fraud Detection

KI ist kein Ersatz für etablierte Prozesse, aber sie wird zum zentralen Verstärker: Sie kann Bildnachweise in großer Menge konsistent bewerten, Muster erkennen, die im Alltag unsichtbar bleiben und so aus einer „reaktiven“ Betrugsprüfung wieder eine proaktive Steuerungsfunktion machen.

# Wie KI bei der Bild-analyse unterstützt

KI kann Bilder automatisiert auf Auffällig-keiten prüfen und Verdachtsindizien in standardisierter Form bereitstellen. Der wichtigste Nutzen liegt in der Skalierung: statt nur Stichproben oder Eskalationsfälle zu prüfen, können Sie grundsätzlich mehr Fälle mit einem ersten Screening versehen. Das ermöglicht:

### Triage

Unauffällige Fälle schneller durchlaufen lassen, auffällige priorisieren.

### Konsistenz

Gleiches Prüfniveau unabhängig von Team, Tageslast oder Erfahrung.

### Entlastung

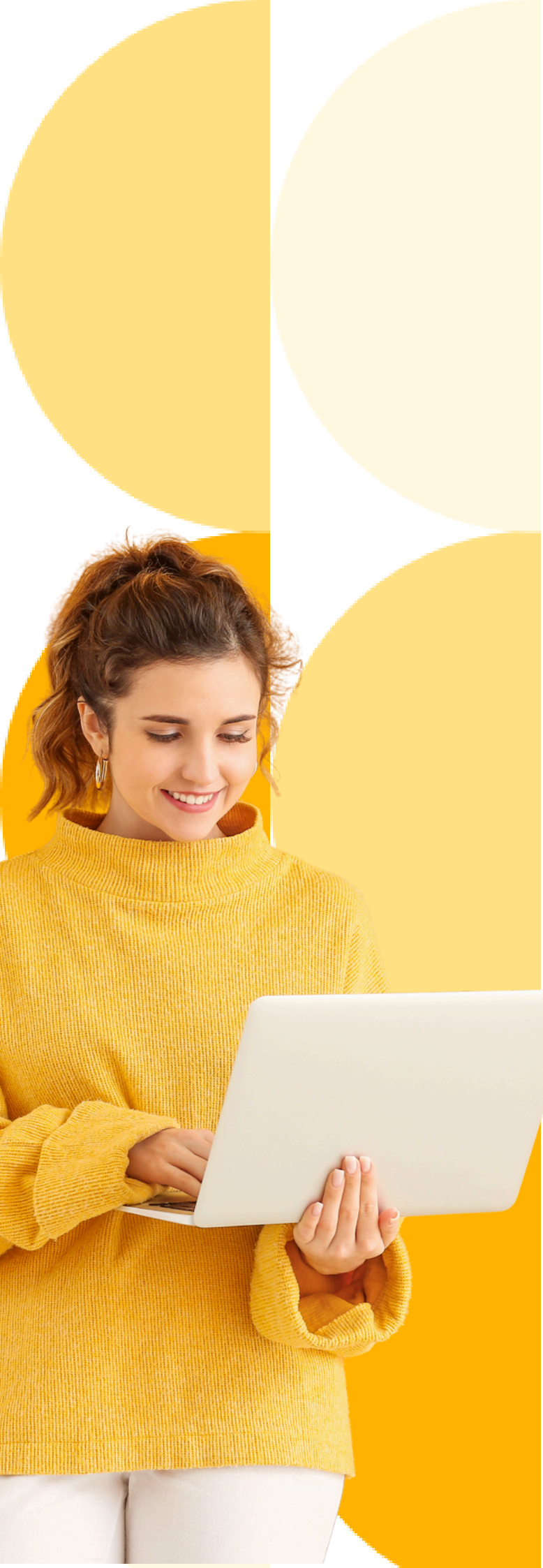
Sachbearbeitung fokus-siert sich auf Entschei-dung und Kommuni-kation, nicht auf foren-sische Detailprüfung.

# Erkennungsansätze: Muster, Artefakte, Metadaten, Kontext

In der Praxis braucht es mehrere Signalebenen:

| | |
|---|---|
| **Pixel-/Inhaltsanalyse (Muster, Texturen, Artefakte):** | Erkennung typischer generativer Spuren wie unplausible Texturen, Kompressionsmuster oder Artefakte, besonders relevant bei KI-generierten Bildern. |
| **Metadatenanalyse** | Kann hilfreich sein, ist aber in realen Kanälen oft unvollständig oder entfernt. Als alleiniger Ansatz daher zu fragil. |
| **Kontext- und Plausibilitätslogik** | Abgleich mit Fallinformationen (Zeit, Ort, Objekt, Historie, Serienmuster). Hier entstehen oft starke Hinweise, aber nicht zwingend „im Bild“. |

Moderne Fraud Detection wird belastbar, wenn diese Ebenen kombiniert werden: Bildsignale für Authentizität, Kontextsignale für Plausibilität und Prozesssignale für Priorisierung.



# Warum eine Kombination aus Mensch und Maschine ideal ist

Die beste Wirkung entsteht, wenn KI die Vorarbeit übernimmt und Menschen die Entscheidung treffen:

- KI liefert skalierbare, konsistente Hinweise (z. B. Score/Flag), auch bei hohem Durchsatz.
- Menschen bewerten Grenzfälle, klären Widersprüche und steuern die Kommunikation mit Kundinnen und Kunden.
- Gemeinsam reduzieren Sie sowohl False Negatives (Leakage) als auch False Positives (unnötige Reibung).

Wichtig ist dabei das Zielbild: KI nicht als „Black-Box-Entscheider“, sondern als Entscheidungsunterstützung, die Triage und Eskalation sauber in bestehende Rollen (Schaden, SIU, Compliance) integriert.

# 06

## Flixcheck Verify – Überblick über die Lösung

Flixcheck Verify adressiert genau die Praxislücke, die durch generative KI entstanden ist: Es liefert spezialisierte Bildsignale zur Erkennung synthetischer und manipulierter Inhalte – automatisiert, skalierbar und so konzipiert, dass es in reale Schadenprozesse passt.

# Was ist Flixcheck Verify?

Flixcheck Verify ist eine Lösung zur automatisierten Erkennung von Bildmanipulationen und KI-generierten Inhalten in Uploads. Der Fokus liegt darauf, Schadennachweise und bildbasierte Dokumente frühzeitig auf Auffälligkeiten zu prüfen und der Sachbearbeitung verwertbare Hinweise zu liefern.
Kernbausteine sind:

**Detect AI-Generated Images:**

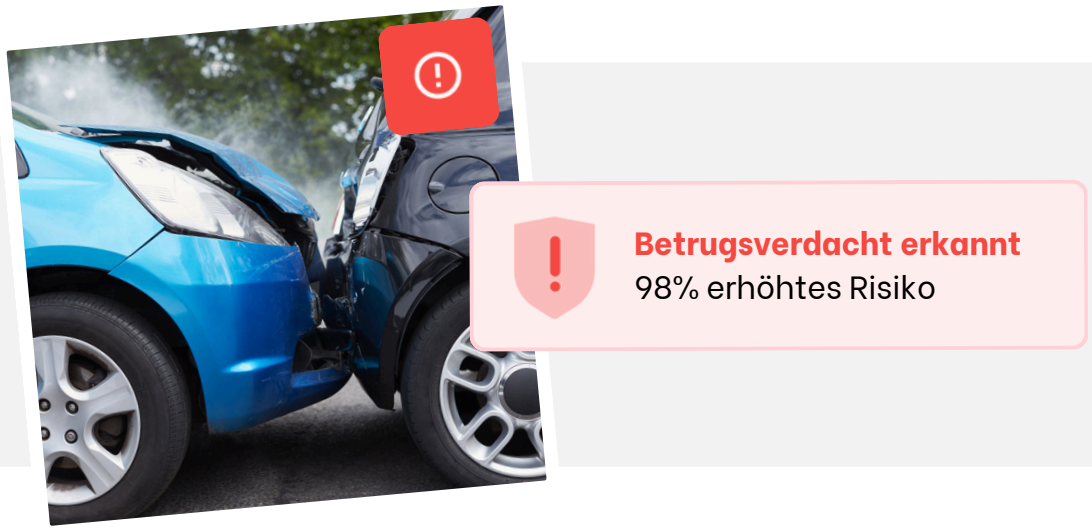
Erkennt, ob ein Bild vollständig synthetisch erzeugt wurde. Die Erkennung basiert auf Pixel- und Inhaltsanalyse (Form, Textur, Kompression, Artefakte) und funktioniert ohne Wasserzeichen und unabhängig von Metadaten auch dann, wenn EXIF-Daten fehlen oder entfernt wurden.

**Detect Deepfakes:**

Erkennt Deepfakes in Bildern und Videos mit Schwerpunkt auf Gesichtsmanipulation (z. B. Face Swaps, Gesichtstransformationen) und liefert einen Deepfake-Score als Wahrscheinlichkeit, dass ein Gesicht manipuliert wurde.

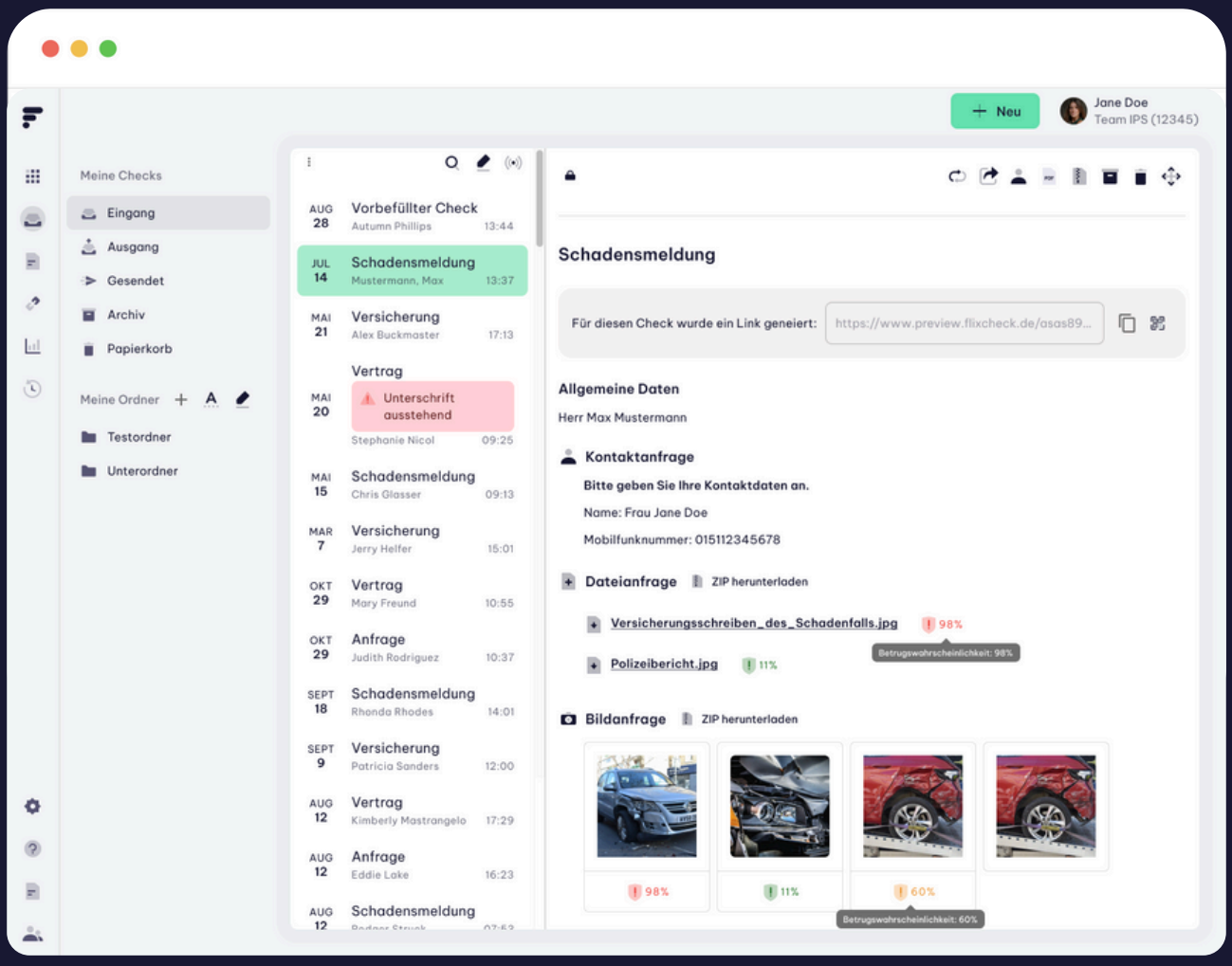
Damit wird die zentrale Abgrenzung operational nutzbar:

- „Ist das Bild komplett synthetisch?“ (AI-Generated Images)
- „Wurde ein reales Bild/Video synthetisch manipuliert – insbesondere im Gesicht?“ (Deepfakes)



# Positionierung im Flixcheck-Ökosystem

Flixcheck Verify ergänzt digitale Datenerfassung und Upload-Prozesse um eine Sicherheits- und Vertrauensebene. Überall dort, wo Bilder oder Dokumente in digitale Abläufe einfließen z. B. in strukturierten Checks oder kanalübergreifenden Uploads kann Verify als automatisierter Prüfschritt eingesetzt werden: zur Triage, zur Markierung von Auffälligkeiten und zur Unterstützung der Sachbearbeitung.



# Ziele von Flixcheck Verify

### Frühzeitige Erkennung von KI-Betrug

Statt erst im Nachgang durch Stichproben oder Auffälligkeiten im Prozess zu reagieren, ermöglicht Verify ein frühes Screening direkt beim Eingang von Bildnachweisen. Gerade bei KI-generierten Bildern ist das entscheidend, weil visuelle Plausibilität heute kein verlässliches Kriterium mehr ist.

### Entlastung der Schadenbearbeitung

Verify reduziert den Bedarf, jedes Bild manuell „forensisch“ prüfen zu müssen. Die Sachbearbeitung erhält konsistente Signale (z. B. synthetisch/echt bzw. Deepfake-Score) und kann ihre Zeit auf Klärung, Kommunikation und Entscheidung verwenden statt auf zeitintensive Sichtprüfungen ohne Trennschärfe.

### Reduktion finanzieller Schäden

Durch bessere Triage und weniger Leakage sinkt das Risiko unberechtigter Auszahlungen, besonders relevant bei skalierbaren Serienmustern, bei denen ein einzelnes funktionierendes KI-Muster schnell in viele Varianten übersetzt werden kann.

# Hosting & Datenhaltung

Zur automatisierten Betrugserkennung in sensiblen Kundenprozessen nutzt Flixcheck die Services von **Sightengine**. Um höchste Datenschutzanforderungen zu erfüllen, verarbeitet Sightengine sämtliche Daten ausschließlich innerhalb der Europäischen Union – konkret an Serverstandorten in Irland, Frankreich und Deutschland. Für das Hosting setzt Sightengine auf ausgewählte europäische Infrastrukturpartner:

- **OVH SAS** (Frankreich) stellt dedizierte Server zur Verfügung,
- **Amazon Web Services** (AWS) betreibt Dienste wie EC2, RDS und S3 in Irland und Frankreich,
- **Hetzner Online GmbH** (Deutschland) sorgt für performante, DSGVO-konforme Serverinfrastruktur auf deutschem Boden.

Durch diese Konstellation ist gewährleistet, dass sämtliche Verarbeitungsschritte sowohl technisch als auch vertraglich auf europäische Datenschutzstandards ausgerichtet sind, ein zentrales Kriterium für Unternehmen in regulierten Branchen.

# 07

## Fazit

KI-gestützter Betrug ist keine theoretische Zukunftsfrage mehr, sondern eine reale Verschiebung der Angriffsfläche im Schadenmanagement: Bilder lassen sich heute in hoher Qualität erzeugen oder manipulieren – schnell, variantenreich und oft ohne klassische Spuren.

Das trifft auf Schadenabteilungen, die unter Zeitdruck und hoher Auslastung arbeiten und in heterogenen Kanälen mit wechselnder Bildqualität entscheiden müssen.

**Die Konsequenz ist klar: Versicherer brauchen zusätzliche, spezialisierte Signale, die direkt im Bild ansetzen, robust auch ohne Metadaten, skalierbar über große Fallmengen und so integriert, dass Entscheidungen nachvollziehbar und DSGVO-konform bleiben.**

Flixcheck Verify unterstützt genau an dieser Stelle: mit automatisierter Erkennung KI-generierter Bilder (pixel-/inhaltsbasiert, ohne Wasserzeichen und unabhängig von Metadaten) sowie Deepfake-Erkennung für Gesichtsmanipulationen inklusive Score. So lassen sich Fälle frühzeitig triagieren, Sachbearbeitung entlasten und finanzielle Schäden reduzieren ohne das Kundenerlebnis unnötig zu belasten.

Wenn Sie schnelle, digitale Schadenprozesse weiterhin ermöglichen und gleichzeitig die neue Betrugsdimension beherrschbar machen wollen, ist jetzt der richtige Zeitpunkt, Fraud Detection strategisch zu erweitern und Bildauthentizität als festen Bestandteil der Schadenstrategie zu verankern.

**Jetzt beraten lassen!**