

ABBYY

E-BOOK
FINANZDIENSTLEISTUNGEN

Banken setzen auf Intelligenz:

Wie KI und ML Banken dabei
helfen, Cyberkriminellen und
Compliance-Bestimmungen
einen Schritt voraus zu sein

Inhaltsverzeichnis

Wo das Geld ist	3
Die Weiterentwicklung der Finanzkriminalität	5
Aus Sicht der Compliance: Erfüllung der KYC- und AML-Anforderungen	8
Mit speziell entwickelter intelligenter Automatisierung einen Schritt voraus sein	11
Dokumentenintegrität	13
Prozessintegrität	14
Kontinuierliches	15
Lernen	16

Wo das Geld ist

Als der berühmte amerikanische Bankräuber Willie Sutton gefragt wurde, warum er Banken ausgeraubt hat, antwortete er: „Weil dort das Geld ist.“

Noch heute sind Banken der Ort, wo „das Geld ist“. Aber die kriminellen Techniken haben sich verändert und sind weit entfernt von den bewaffneten Raubüberfällen, für die Sutton bekannt war. Die Finanzkriminalität ist nun digital. Cyberkriminelle erfinden schneller neue Methoden für Betrug und Geldwäsche, als Banken Gegenmaßnahmen ergreifen können.

Laut einem [Bericht von IBM](#) gehören Finanzdienstleistungen nach wie vor zu den Branchen, in denen Datenverstöße am teuersten sind. Der durchschnittliche Schaden pro Verstoß beläuft sich auf 5,56 Millionen US-Dollar.

Im Jahr 2025 wurden laut dem FBI (USA) mehr als

**262 Millionen
Dollar**

durch Kontoübernahmen (ATO) und KI-gestützte Phishing-Betrügereien verloren.

🔗 Quelle



Die europäischen Know-Your-Customer- (KYC) und Anti-Money-Laundering- (AML) Regelwerke haben ihren Ursprung in frühen EU-Initiativen zur Bekämpfung von Finanzkriminalität, wurden jedoch durch die aufeinanderfolgenden EU-Geldwäscherichtlinien (AMLD) sowie das neue europäische AML-Regulierungspaket erheblich gestärkt. Diese Maßnahmen erweiterten formal die Vorgaben zur Bekämpfung der Terrorismusfinanzierung (CFT), harmonisierten Sorgfaltspflichten und Transparenzanforderungen in allen Mitgliedstaaten und etablierten ein einheitliches europäisches AML/KYC-Rahmenwerk – einschließlich einer zentralen europäischen Aufsichtsbehörde (AMLA) zur Sicherstellung konsistenter Durchsetzung und grenzüberschreitender Aufsicht.

Die Nichteinhaltung dieser Vorschriften kann teuer werden – sowohl für den Ruf von Banken als auch für ihre **Finanzergebnisse**. Finanzaufsichtsbehörden in Europa haben in den letzten Jahren zahlreiche hohe **Bußgelder und Sanktionen** für Verstöße gegen Anti-Geldwäsche- (AML) und KYC-Pflichten verhängt, darunter etwa Millionensummen gegen große Institute wie eine führende Bank in Deutschland oder gegen Nicht-Bank-Dienstleister wegen unzureichender Kundenidentifizierung und Transaktionsüberwachung. Diese Maßnahmen zeigen, dass AML/KYC-Compliance ernst genommen wird und Verstöße erhebliche **finanzielle und reputationsbezogene Risiken** bergen können.

Um raffinierte Verbrechen zu verhindern, braucht es raffinierte Maßnahmen. Glücklicherweise erhalten Banken dank der heutigen, auf künstlicher Intelligenz basierenden Technologien die benötigte Transparenz über ihre Prozesse und Inhalte, um die KYC/AML/CFT-Vorschriften einzuhalten und sich flexibel an sich ändernde Bedingungen anzupassen.

Die Weiterentwicklung der Finanzkriminalität

Aufgrund des verschärften Wettbewerbs und der sich wandelnden Kundenerwartungen verlassen sich Finanzinstitute zunehmend auf Automatisierung, mobile Technologie und kontaktlose Interaktionen, insbesondere seit Ausbruch der COVID-19-Pandemie. Diese Maßnahmen bieten zwar erhebliche Vorteile in Bezug auf Produktivität und Kundenzufriedenheit, können jedoch auch neue Schwachstellen schaffen, die Cyberkriminelle ausnutzen können – was sie auch tun.

Neu ist vor allem die Geschwindigkeit und Raffinesse dieser Angriffe. Kriminelle Gruppen nutzen heute automatisierte Angriffe sowie KI-gestützte Identitätsübernahmen, um Gelder innerhalb von Minuten über Konten und Plattformen hinweg zu verschieben und zu waschen. Gleichzeitig haben Aufsichtsbehörden und Banken Schwierigkeiten, Kontrollmechanismen anzuwenden, die ursprünglich für deutlich langsamere Systeme konzipiert wurden.

Das Ergebnis ist ein Anstieg von Identitätsbetrug, Investitionsbetrug, Erpressung durch Ransomware und komplexen Versuchen, illegale Gelder zu verschleiern. Die Herausforderung für Banken besteht nicht nur darin, verdächtiges Verhalten zu erkennen, sondern dies auch schnell genug zu tun, um tatsächlich etwas bewirken zu können.



Die heutigen Finanzverbrecher haben herausgefunden, wie sie die eigenen Systeme und Prozesse eines Instituts als Mechanismen zum Waschen und Stehlen von Geld nutzen können. Zum Beispiel:

- 1 Digitale Infrastruktur:** Angreifer können auf sensible Kontodaten zugreifen, indem sie den legitimen Zugriff von Mitarbeitern nutzen oder Schwachstellen in Cloud-basierten Diensten aufspüren, die nicht korrekt eingerichtet wurden.
- 2 Prozessautomatisierung** Kriminelle können Lücken in automatisierten Prozessen aufdecken, die bei automatisierten Überprüfungen möglicherweise übersehen werden.
- 3 Kundenidentifikation:** Gestohlene Zugangsdaten und durch KI generierte Identitätsfälschungen ermöglichen es Angreifern, herkömmliche Identitätsprüfungen zu umgehen.
- 4 Kunden-Onboarding:** Cyberkriminelle können mithilfe gefälschter Kundenidentitäten synthetische Konten erstellen.

Die jährlich weltweit gewaschene Geldmenge wird auf

**800 Milliarden
bis**

**2 Billionen
US-Dollar**

geschätzt, ungefähr

2 bis 5% des globalen BIP.

Unter Einbeziehung der
durch Betrug Entstehenden
Folgekosten

verlieren

**Finanzinstitute für
jeden Dollar, der
durch Betrug verloren
geht, 5 weitere Dollar.**

↳ Quelle

Was können Finanzinstitute gegen diese ständigen Angriffe unternehmen?

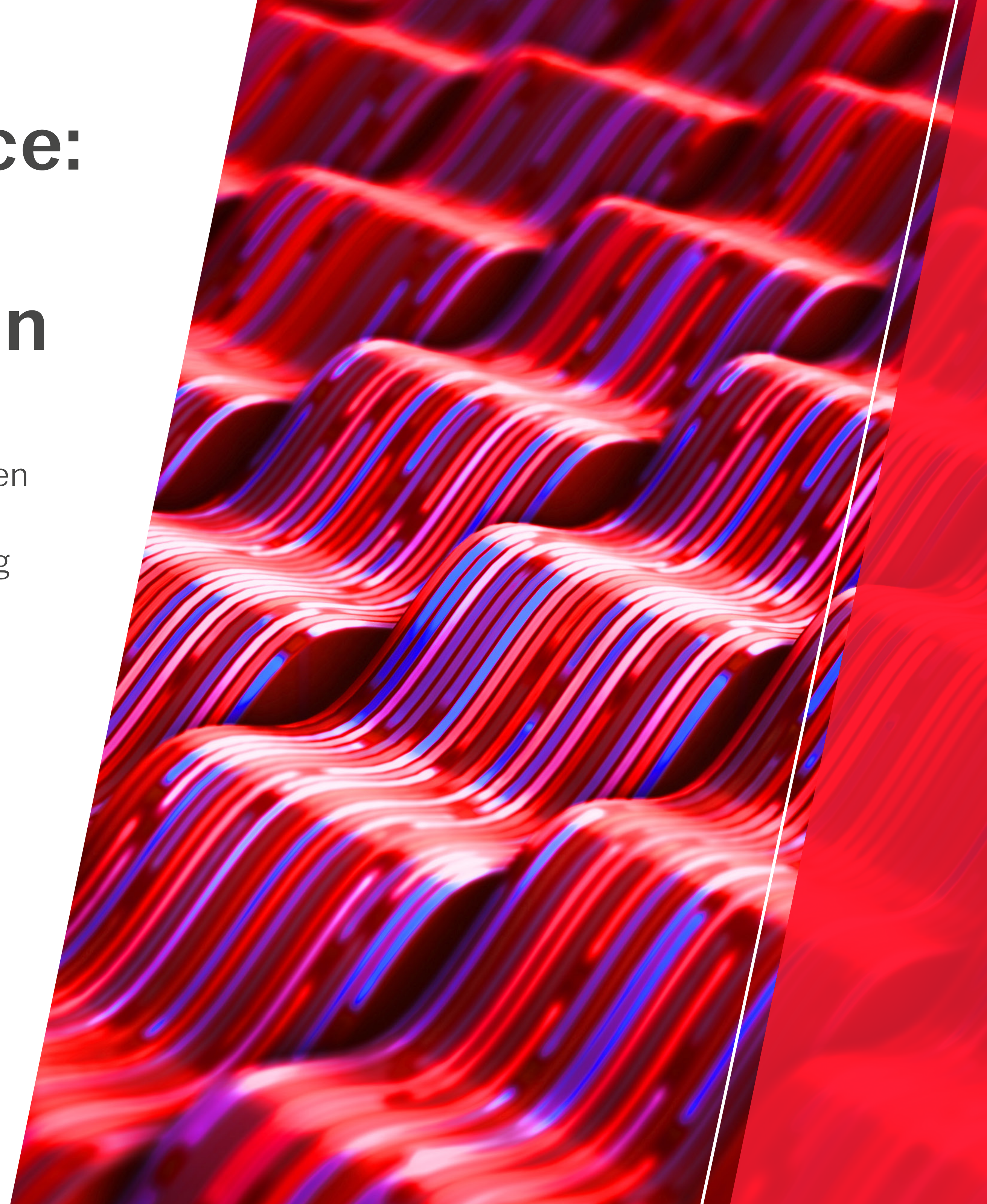
Manuelle Überwachung kann unterstützend wirken, doch allein auf menschliche Kontrolle zu setzen reicht nicht aus, um mit Systemen Schritt zu halten, die in Maschinengeschwindigkeit arbeiten. Manuelle Prüfprozesse sind insbesondere durch folgende Faktoren begrenzt:

- Die Tatsache, dass menschliche Mitarbeiter nicht in der Lage sind, mit dem Umfang und der Geschwindigkeit der Transaktionen rund um die Uhr Schritt zu halten.
- Lücken in der Transaktionsüberwachung und -berichterstattung, durch die verdächtige Aktivitäten nicht in Echtzeit erkannt werden
- Ein erhöhtes Risiko eines menschlichen Fehlers in stressintensiven Arbeitsumgebungen
- Die dauerhafte Herausforderung, Mitarbeitende kontinuierlich über die neuesten kriminellen Methoden zu schulen
- Das Risiko, dass Mitarbeitende selbst in Finanzkriminalität verwickelt sind

Aus Sicht der Compliance: Erfüllung der KYC- und AML/CFT-Anforderungen

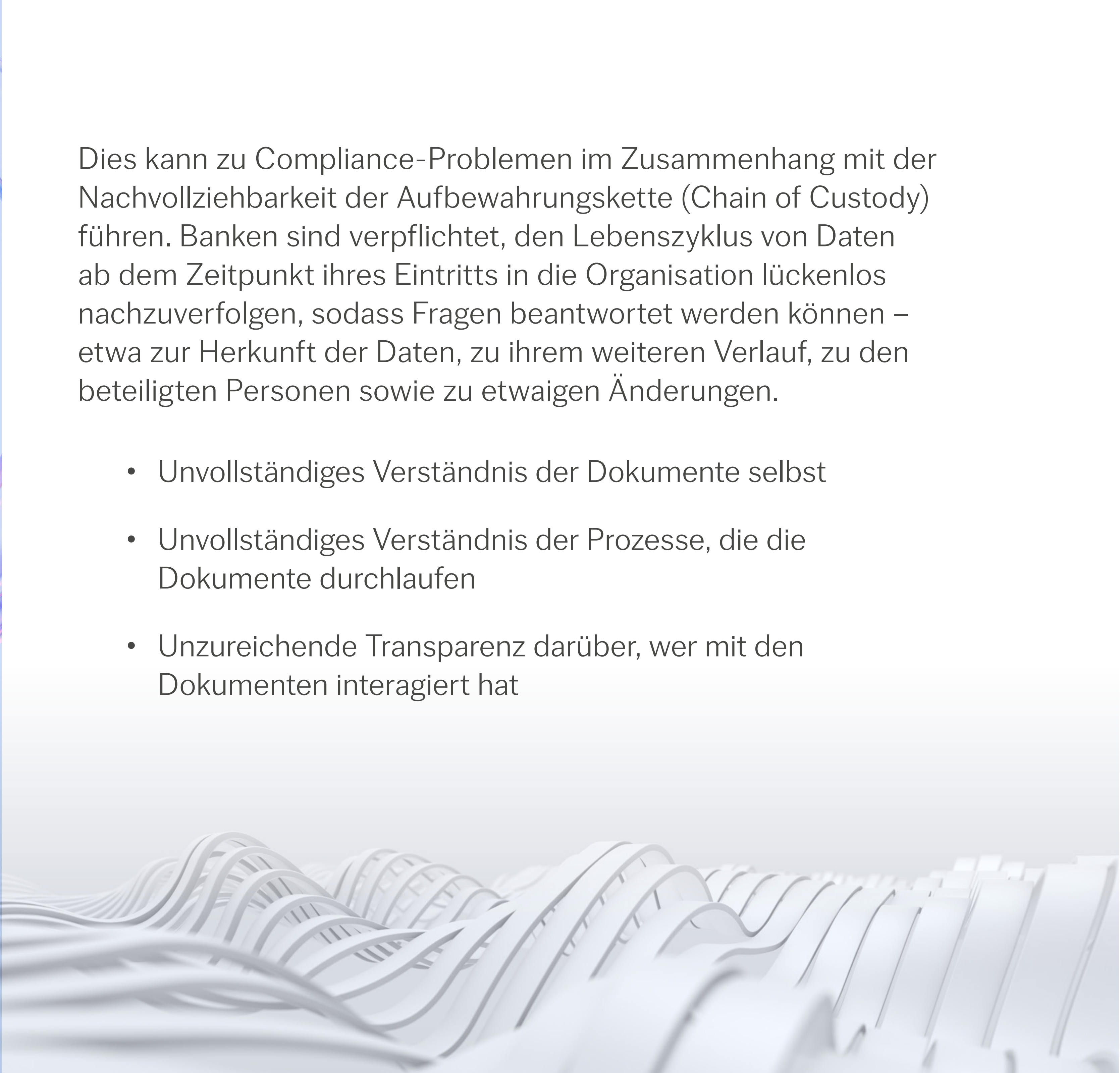
Um die Anforderungen der KYC- und AML-Vorschriften zu erfüllen, müssen Finanzinstitute nachweisen, dass sie Kunden identifizieren, Transaktionen kontinuierlich überwachen und verdächtige Aktivitäten über automatisierte Prozesse hinweg erkennen und entsprechend darauf reagieren können.

Während viele Banken für strukturierte Daten bereits über etablierte Verifizierungsprozesse und führende Aufzeichnungssysteme verfügen, werden Kunden- und Transaktionsdaten häufig in Dokumenten erfasst, die sich mit nur geringer Transparenz durch die Organisation bewegen. In der Folge gehen die Verknüpfungen zwischen den Daten, den Prüfprozessen und den daraus abgeleiteten Entscheidungen oft verloren.





Dies kann zu Compliance-Problemen im Zusammenhang mit der Nachvollziehbarkeit der Aufbewahrungskette (Chain of Custody) führen. Banken sind verpflichtet, den Lebenszyklus von Daten ab dem Zeitpunkt ihres Eintritts in die Organisation lückenlos nachzuverfolgen, sodass Fragen beantwortet werden können – etwa zur Herkunft der Daten, zu ihrem weiteren Verlauf, zu den beteiligten Personen sowie zu etwaigen Änderungen.

- Unvollständiges Verständnis der Dokumente selbst
 - Unvollständiges Verständnis der Prozesse, die die Dokumente durchlaufen
 - Unzureichende Transparenz darüber, wer mit den Dokumenten interagiert hat
- 

Beispiel: Kunden-Onboarding

Wenn ein Kunde im Rahmen des Onboarding-Prozesses einen Führerschein einreicht, sollte in einem Chain-of-Custody-Protokoll angegeben werden, wann und wie das Dokument gescannt wurde, wie die Daten extrahiert und überprüft wurden, was mit dem gescannten Bild nach dem Onboarding passiert ist und wie die extrahierten Daten bis zum Dokument zurückverfolgt werden können. Lücken in dieser Kette können nicht nur zu KYC-Verstößen führen, sondern auch zu Sicherheitslücken, die von Cyberkriminellen ausgenutzt werden können.

Das Kunden-Onboarding, bei dem die Bank erstmals die Identität des Kunden anhand von Dokumenten feststellt, ist der entscheidende erste Schritt, um die Einhaltung der KYC-Richtlinien zu gewährleisten.

ABBYY



Die weltweiten Ausgaben für AML-Systeme von Drittanbietern werden bis 2028 voraussichtlich

**51,7
Milliarden \$**

erreichen.

↳ Quelle

Mit speziell entwickelter intelligenter Automatisierung einen Schritt voraus sein

Um die KYC- und AML-Vorschriften einzuhalten und gleichzeitig kriminelle Aktivitäten zu verhindern, die von den Compliance-Anforderungen möglicherweise nicht abgedeckt werden, müssen Finanzinstitute zunächst über die Möglichkeit verfügen, Dokumente zu überprüfen, um versuchten Betrug aufzudecken. Außerdem benötigen sie Transparenz über ihre Prozesse. Diese muss eine kontinuierliche Überwachung auf Unregelmäßigkeiten ermöglichen, die auf betrügerisches Verhalten hinweisen könnten.

Darüber hinaus benötigen sie Einblicke in die Weise, wie Menschen mit den Prozessen und Dokumenten interagieren, die auf verdächtiges Verhalten hinweisen könnte. Dieser Ansatz wird Banken mit der benötigten Digital Intelligence ausstatten, um sich sowohl vor Betrug als auch vor Verstößen gegen Vorschriften zu schützen.



Führende Banken betrachten Dokumente heute als aktive Quellen für risikorelevante Erkenntnisse. Durch den Einsatz speziell entwickelter KI und intelligenter Automatisierung zur Extraktion, Klassifizierung und Validierung von Informationen bereits beim Eingang in die Organisation können Finanzinstitute Inkonsistenzen und Anomalien sofort und kontinuierlich erkennen – ohne ihre Mitarbeitenden operativ zusätzlich zu belasten.

Die wirkungsvollsten Automatisierungsprogramme setzen auf speziell entwickelte Document-AI-Lösungen, um Dokumente, Prozesse und Nutzeraktivitäten in einer einheitlichen Sicht zusammenzuführen. Mit in dokumentengetriebene Workflows integrierter Intelligenz erhalten Banken transparente Einblicke in Entscheidungsprozesse und Informationsflüsse, können die Betrugserkennung stärken und zugleich die Einhaltung der Anforderungen an die Nachvollziehbarkeit der Aufbewahrungskette nachweisen.





Dokumentenintegrität

Obwohl die Finanzbranche die digitale Transformation immer mehr umsetzt, stammen viele Kundendaten von Banken aus Dokumenten: Identifikationsformulare, Unternehmensnachweise, Kreditanträge, Steuererklärungen usw. Wenn Finanzinstitute Betrug verhindern und ihren Compliance-Verpflichtungen nachkommen möchten, müssen sie jedes Kundendokument zuverlässig auf Unregelmäßigkeiten prüfen können, die auf kriminelle Absichten hinweisen könnten. Sie müssen auch eine direkte Verknüpfung zwischen ihren Aufzeichnungssystemen für die KYC/AML- Einhaltung und ihren Kundeninteraktionen herstellen, vom Onboarding über ganze Customer Journeys.

Document AI extrahiert und validiert Informationen bereits beim Eingang in die Organisation und verknüpft die Inhalte eines Dokuments direkt mit KYC- und AML-Systemen zur Überwachung der Aufbewahrungskette. Dadurch sind Banken in der Lage, Kundendaten ab dem Zeitpunkt ihres Eintritts in die Organisation über den gesamten Lebenszyklus hinweg bis hin zum Offboarding nachzuverfolgen. Fordert ein Compliance-Beauftragter entsprechende Chain-of-Custody-Nachweise an, kann das Finanzinstitut jeden einzelnen Berührungspunkt lückenlos dokumentieren.



Prozessintegrität

Sobald Kundendaten in ein Finanzinstitut eingehen, sei es über Dokumente oder aus digitalen Quellen, werden sie zur Basis für eine beliebige Anzahl von Prozessen, einschließlich Kunden-Onboarding, Compliance-Prüfungen, Kreditgenehmigungen und vielem mehr. Die meisten Banken haben eine gute Vorstellung davon, wie diese Prozesse ablaufen sollen. Doch die Lücken zwischen Theorie und Praxis können größer sein als sie denken – und Möglichkeiten für Betrug oder Datendiebstahl bieten.

Process Intelligence nutzt Daten aus digitalen und physischen Quellen, um Banken einen Einblick in die tatsächliche Ausführung ihrer Prozesse von Anfang bis Ende zu geben. Durch das Sammeln und Analysieren der von Informationssystemen generierten Zeitstempeldaten können erweiterte Algorithmen einen „digitalen Zwilling“ von Geschäftsabläufen und -prozessen erstellen. Diese visuellen Modelle bieten detaillierte Einblicke in die tägliche Ausführung von Prozessen – vom „Standard“- oder „Ideal“- Pfad bis hin zu allen anderen Variationen.

Im Kampf gegen Betrug und Geldwäsche kann Process Intelligence Unregelmäßigkeiten in der Datenverarbeitung aufdecken, die von Cyberkriminellen ausgenutzt werden könnten. Zudem ermöglicht sie eine kontinuierliche (24/7) Überwachung von Prozessen auf potenzielle Sicherheitslücken und benachrichtigt Prozessverantwortliche automatisch, wenn ein sofortiges Eingreifen erforderlich ist. Darüber hinaus sind Banken in der Lage, den Lebenszyklus von Kunden- und Transaktionsdaten nachzuverfolgen, während diese gemeinsam mit ihren zugehörigen Dokumenten durch und zwischen Prozessen fließen, und bei Bedarf eine präzise und nachvollziehbare Dokumentation der Aufbewahrungskette bereitzustellen.



Kontinuierliches Lernen

Compliance und Betrugsprävention sind in ständigem Wandel, da laufend neue Vorschriften entstehen und Kriminelle neue Betrugsmaschen finden. Document-AI- und Process-AI-Lösungen sind sehr anpassungsfähig, wenn sich die Bedingungen sowie Compliance-Vorschriften und -Richtlinien ändern. Mithilfe von Machine Learning können diese Lösungen aus jeder Iteration lernen und sich entsprechend anpassen.

Ausblick

Während Banken und andere Finanzinstitute ihre digitale Transformation weiter vorantreiben, entstehen zugleich neue Risiken. Moderne Cyberkriminelle wissen, wie sie die digitale Infrastruktur eines Unternehmens gezielt ausnutzen können, um Betrug und Datendiebstahl zu begehen. Die Erkennung solcher Aktivitäten ist komplexer geworden, und um einen Schritt voraus zu bleiben, sind intelligente Werkzeuge erforderlich.

KI-gestützte Lösungen spielen heute eine zentrale Rolle bei der skalierbaren Überwachung von Hunderten von Prozessen und Tausenden von Dokumenten. Sie ermöglichen es, potenzielle kriminelle Aktivitäten schnell und präzise zu identifizieren. Diese Systeme ersetzen nicht das menschliche Urteilsvermögen, sondern entlasten Compliance- und Betrugspräventionsexpertinnen und -experten von routinemäßigen Kontrollaufgaben, sodass sie sich auf risikoreichere Fälle konzentrieren können.

Die Kombination aus menschlichem Fachwissen und einer digitalen Belegschaft, die Finanzinstituten hilft, schnell zu skalieren und sich anzupassen, um die KYC- und AML-Vorschriften einzuhalten und gleichzeitig ihre eigene Abwehr gegen Cyberkriminalität zu stärken – heute, morgen und in den nächsten Jahren.



Möchten Sie mehr sehen?

Wenden Sie sich an einen ABBYY-Experten, um eine Demo von ABBYY Document AI für die Einhaltung von KYC- und AML-Vorschriften zu erhalten.

Weitere Informationen finden Sie unter: **[www.ABBYY.com/finserv](https://www.abbyy.com/finserv)**

Kontaktieren Sie unsere Niederlassungen auf der ganzen Welt: **[www.ABBYY.com/contacts](https://www.abbyy.com/contacts)**



© ABBYY 2025. ABBYY ist ein eingetragenes Warenzeichen oder Warenzeichen von ABBYY Development Inc. und/oder seinen verbundenen Unternehmen. Dies betrifft auch das Logo, Produkt- oder Firmennamen (oder Teile davon) von ABBYY Development Inc. und/oder seiner verbundenen Unternehmen: sie dürfen nicht ohne Zustimmung ihrer jeweiligen Besitzer genutzt werden. Alle anderen hierin erwähnten Produktnamen und Markenzeichen sind Eigentum ihrer jeweiligen Inhaber. DS-1331

www.abbyy.com