



ABBYY

EBOOK

Trusted Documents for AI-Driven Decisions

Why document integrity is the
foundation of fraud prevention,
compliance, and automated
decisioning

Table of contents

Executive summary	3
Document fraud today: 5 key insights	4
Documents are the front door—and fraud knows it	6
The new generation of document fraud	8
One fraudulent document: Multiple consequences	9
Stop fraud before it enters the process	10
Three layers of protection	11
FRAML convergence: Fraud and AML as a unified control	12
Where document fraud happens—and what it costs	13
A framework for evaluating your approach	14
Trust starts at the front door	15

Executive summary

Digital transformation has redefined how organizations process documents, with workflows and AI-driven decisioning driving efficiency, but also heightening document integrity risks. Fraud now focuses on the document layer—manipulated bank statements, paylips, invoices, and IDs that can enter systems undetected, triggering approvals or payments. Once fraudulent documents enter operational systems, their impact extends beyond the original transaction—affecting investigations, compliance reporting, and even the quality of data feeding AI models.

At the same time, regulatory expectations are evolving. Financial institutions and other regulated organizations must demonstrate not only that fraud controls exist but also that verification decisions are explainable, auditable, and consistently applied across digital channels.

As a result, leading organizations are shifting their fraud prevention strategies upstream. Instead of detecting fraud only after suspicious activity occurs, they are establishing document trust at the point of ingestion—verifying authenticity before document data informs any decision. This shift reflects a broader transformation in financial crime management, including the convergence of fraud and anti-money-laundering controls into unified FRAML frameworks.

Organizations that embed document integrity into the front of their processes can reduce fraud exposure, improve operational efficiency, and meet increasingly complex regulatory expectations. This ebook provides a framework for achieving this.

Document fraud today: 5 key insights

1 Documents are becoming the primary fraud attack surface.

As onboarding and transactions move online, documents submitted through digital channels are now the primary entry point for fraud. Fraudsters increasingly manipulate the documents that authorize transactions rather than targeting the transactions themselves.

2 Traditional verification methods are no longer sufficient.

Manual review and rule-based validation were designed to confirm the presence of expected information, not to detect modern digital manipulation. Techniques such as metadata tampering, font substitution, and layer manipulation often leave no visible evidence during visual inspection.



3 The cost of document fraud extends beyond financial loss.

Fraudulent documents create cascading operational and compliance consequences, including investigation backlogs, regulatory exposure, and corrupted data feeding risk models and AI decision systems. In U.S. financial services, every **\$1 of fraud loss generates \$5.75 in total cost** when operational and compliance impacts are included.

4 Fraud prevention must move upstream.

Detecting fraud after a document has already informed a decision is no longer sufficient. Organizations are shifting toward verification at document ingestion, ensuring that authenticity checks occur before document data enters operational or analytical systems.

5 Document integrity is becoming a foundation of FRAML strategies.

Fraud prevention and anti-money-laundering programs are converging into integrated financial crime frameworks. Reliable document verification provides the shared foundation both functions require to maintain consistent risk controls across the customer lifecycle.



Documents are the front door— and fraud knows it

Documents are the entry point for critical decisions across every industry. Loan approvals, insurance claims, government programs, vendor onboarding, and compliance checks all begin with documents submitted from external sources. These submissions influence who gets credit, which claims are paid, and access to regulated services.

Digital onboarding and remote submissions have replaced in-person checks, increasing both convenience and the attack surface. Documents now flow in through a dozen digital channels, introducing new risks. Fraudsters target these processes, manipulating statements, invoices, or identification documents to enable unauthorized transactions.

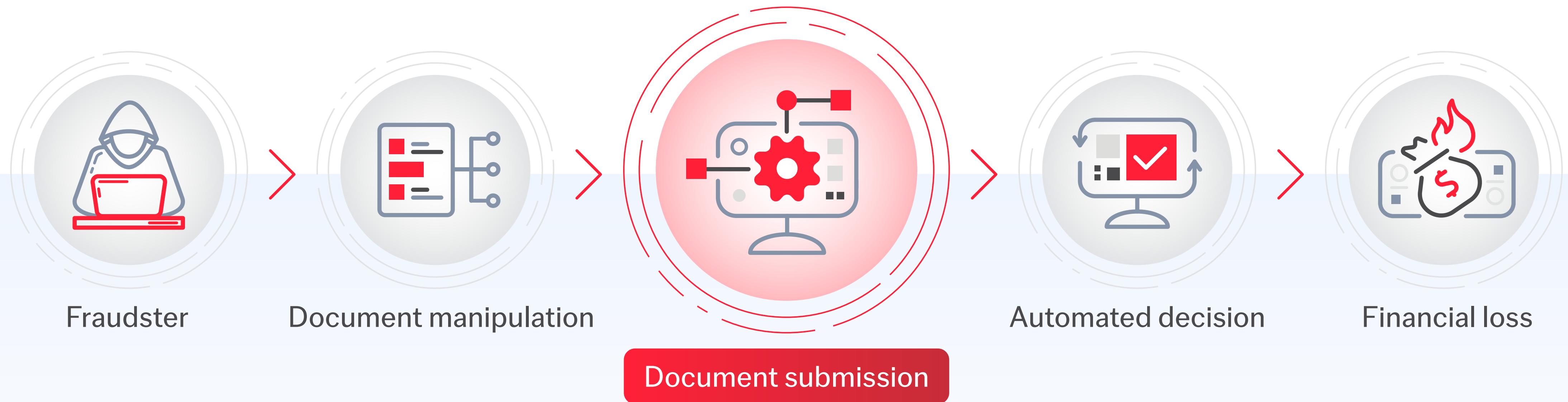
Despite this shift, many verification methods remain manual or focused solely on data extraction rather than authenticating the file itself. Fraud schemes exploit these gaps. The impact is clear in recent statistics:

\$485.6B in global losses from fraud in 2023 (Nasdaq)	\$5.75 total cost per dollar of fraud in U.S. financial services (LexisNexis)	44% of North American financial institutions rely primarily on manual fraud detection (LexisNexis)
---	---	--

Every automated decision begins with a document. If that file is fraudulent, the consequences start with ingestion.

Documents are the front door— and fraud knows it

Document fraud life cycle



The new generation of document fraud

Editing tools and generative AI have made creating fraudulent documents easier than ever. Where once a forger needed special expertise, now they can produce altered bank statements, fabricated payslips, synthetic IDs, or repurposed documents quickly, at scale.

Manipulations can range from simple edits—such as changing numbers or names—to deep alterations, including modifying PDF layers, adjusting metadata, or cloning images. These sophisticated tactics leave subtle traces that often bypass manual review but can be detected through forensic analysis.

Why traditional verification falls short.

Manual processes cannot reliably catch subtle alterations, font swaps, or hidden layer changes. Rule-based systems may check required fields but cannot confirm authenticity. Many organizations lack the capability to analyze document structure or integrate fraud detection directly into document workflows, letting manipulated files slip through.



**Metadata
tampering**



**Font
substitution**



**Layer
manipulation**



**Image
cloning**



**Template
reuse**

One fraudulent document: Multiple consequences

Fraud rarely stops with a single transaction. Fake documents can lead to direct financial loss (inflated insurance claims, unauthorized loans), operational disruption, compliance penalties, and data contamination. Research shows every dollar lost to fraud generates \$5.75 in total cost, including investigation and remediation. Fraudulent data can compromise AI systems, risk models, and compliance records, spreading negative effects across the business.

“ The cost of a fraudulent document rarely ends with the transaction it supports.

Stop fraud before it enters the process

Traditional fraud strategies focus on detecting suspicious transactions downstream, but this is no longer effective in high-volume, digital environments. Leading organizations move verification upstream, checking authenticity at the point of document ingestion. This approach enables consistent verification across all channels, producing explainable signals that support investigators and meet regulatory requirements.

Regulatory standards continue to evolve, with new fraud monitoring and documentation requirements in the UK, United States, Australia, and beyond. Organizations must act before decisions—and risks—enter their systems.



Three layers of protection

A comprehensive document fraud strategy includes:

Document Intelligence

Extracts and structures information from submitted files. Advanced validation and routing send uncertain cases to human review.

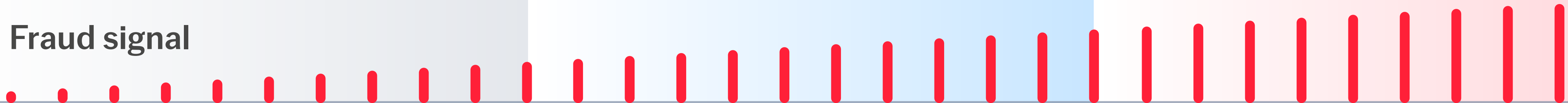
Forensic Analysis

Inspects metadata, layers, and layout to identify signs of tampering, generating explainable risk scores for investigators.

Process Intelligence

Monitors workflow behavior, identifies unusual routing or rule violations, and correlates risk signals with process anomalies.

Fraud signal



Combined, these layers deliver robust, scalable fraud defense.

ABBYY

FRAML convergence: Fraud and AML as a unified control

Financial crime prevention is converging, aligning fraud and anti-money laundering (AML) controls. Modern schemes blend identity manipulation, document forgery, and transaction abuse, requiring integrated oversight. Regulators now demand continuous, cross-functional monitoring, which Process Intelligence enables by monitoring workflows across previously separated silos. Document integrity underpins both fraud and AML frameworks. Without it, financial crime controls cannot scale.

Where document fraud happens—and what it costs

Fraud occurs throughout the business lifecycle. Each instance begins when the manipulated file bypasses authenticity checks.

- **Loan application fraud:** Edited bank statements and fake proof-of-income documents pass undetected, enabling unauthorized credit.
- **Insurance claims fraud:** Repurposed and inflated invoices produce fraudulent payouts.
- **Government benefits fraud:** Altered IDs and mismatched residency documents allow ineligible claims.



A framework for evaluating your approach

Effective fraud detection requires:

- ✓ Authenticity checks at ingestion
- ✓ Metadata, structure, and layout analysis
- ✓ Forensic signals built into workflows
- ✓ Explainable indicators for compliance
- ✓ Support for human review at scale
- ✓ Global coverage for diverse document types
- ✓ Trusted signals fed to fraud and AML systems
- ✓ Insights into workflow behavior and controls

Most organizations find gaps in one or more areas, best addressed by introducing intelligence at the point of document entry.

ABBYY combines Document AI, partner forensic solutions, and Process AI to deliver a trusted front door for document-driven workflows.

Trust starts at the front door

Automation is transforming decisioning, but it only amplifies the quality of the input documents. Moving verification to the start of the process shifts fraud prevention from reactive to proactive.

ABBYY ensures documents are trustworthy as soon as they enter your workflow by combining ABBYY Document AI, partner forensic capabilities, and ABBYY Process AI. This layered approach identifies fraud early, reduces operational risk, and strengthens regulatory compliance.

Organizations that embed document integrity at the front of their workflows detect more fraud, prevent greater losses, and navigate evolving regulations with confidence.

ABBYY



Learn how ABBYY enables trusted document processing.

Request a demo to see how your organization can verify
document integrity at the earliest stage.

For more information visit: **www.ABBYY.com**

Contact our offices worldwide: **www.ABBYY.com/contacts**



© ABBYY 2026. ABBYY is a registered trademark or a trademark of ABBYY Development Inc. and/or its affiliates. This designation can also be logo, product, or company name (or part of any of the above) of ABBYY Development Inc. and/or its affiliates and may not be used without consent of their respective owners. All other product names and trademarks mentioned herein are the property of their respective owners. DS-1767

www.abbyy.com