

TRUEDOC RESEARCH · 2026 EDITION

The Global Document Fraud Report 2026

AI, synthetic documents, and the new economics of forgery — how fake and altered documents became the world's single largest identity-fraud vector, and what risk teams must change before approving the next applicant, loan, vendor, or claim.

\$12.5B

U.S. consumer fraud losses, 2024
(+25% YoY)

50%

of all fraud attempts involve forged or altered documents

+1,100%

growth in deepfake fraud, Q1 2024 → Q1 2025

Fraud went industrial — and documents are the front line

Reported fraud is at an all-time high, and the mechanism behind a growing share of it is deceptively simple: a document that looks real but isn't. In 2024, forged or altered documents became the most common identity-fraud vector worldwide — and generative AI has turned what was once a careful manual craft into something that can be produced in seconds, at scale, for a few dollars.

For most of the last decade, fraud defenses focused on verifying **identities** — matching a person to a government ID. But the documents that flow **after** that check — pay stubs, bank statements, invoices, proofs of address, contracts, and the IDs themselves as images — are now where fraud increasingly lands. These supporting documents drive credit, payout, hiring, rental, and claims decisions, yet they are the layer most identity systems were never designed to forensically inspect.

This briefing synthesizes the most recent public data from the U.S. Federal Trade Commission, the FBI's Internet Crime Complaint Center, FinCEN, Sumsub, Deloitte, and Regula to map the scale of the problem, the role of AI, and what a defensible 2026 document-verification program looks like.

\$12.5B

U.S. consumer fraud losses in 2024 — up 25% over 2023, a record high

FTC CONSUMER SENTINEL DATA BOOK 2024

\$16.6B

Reported to the FBI's IC3 in 2024 (+33% YoY); 83% from cyber-enabled fraud

FBI IC3 2024 INTERNET CRIME REPORT

50%

of all fraud attempts in 2024 involved forged or altered documents — the #1 type

SUMSUB IDENTITY FRAUD REPORT

\$40B

projected U.S. generative-AI fraud losses by 2027, from \$12.3B in 2023 (32% CAGR)

DELOITTE CENTER FOR FINANCIAL SERVICES

The shift in one sentence

Identity verification asks **"is this the right person?"** — document forensics asks **"is this document real?"** In 2026, the second question is where the losses are, and answering it now requires layered forensic and AI-generation analysis, not a human glance.

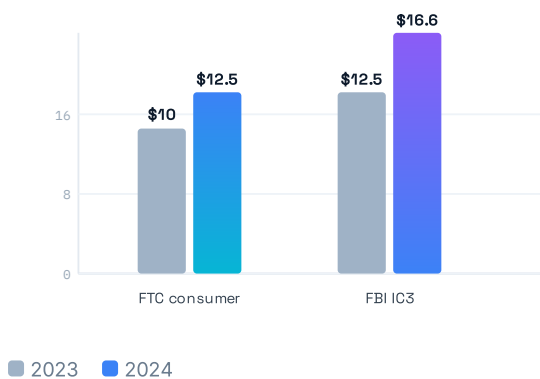
01 The scale of the problem

Fraud losses are not just high — they are accelerating. Two independent U.S. authorities recorded record totals in 2024, and the underlying reporting from financial institutions confirms the trend is structural, not a one-year spike.

The FTC's Consumer Sentinel Network logged **\$12.5 billion** in reported consumer fraud losses in 2024 — a 25% jump over 2023. Notably, the number of reports stayed flat; what rose was the share of victims who actually lost money, from 27% to 38%. Separately, the FBI's Internet Crime Complaint Center recorded a record **\$16.6 billion** in losses, up 33% year over year, with cyber-enabled fraud responsible for 83% of the total. Business email compromise alone accounted for \$2.77 billion.

Reported fraud losses are climbing fast

U.S. losses, 2023 vs 2024 (USD billions)



Source: FTC Consumer Sentinel 2024; FBI IC3 2024

+110%

Increase in fraud-related Suspicious Activity Reports filed by U.S. financial institutions between 2020 (552,920) and 2024 (1,165,642).

Source: FinCEN, via U.S. Federal Reserve Consumer Compliance Outlook (2025)

The institutional data mirrors the consumer data: more reports, larger losses, and a rising share of incidents that succeed. Critically, the FTC notes the jump was driven less by *more* fraud attempts and more by attempts that **worked** — a signal that attacker tooling, much of it AI-assisted, is getting better faster than defenses.

These figures capture only *reported* incidents in the United States; true global losses are materially higher. They establish the backdrop for the central finding of this report: a large and growing share of this fraud is executed through documents.

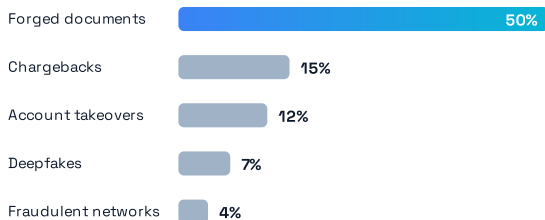
02 Documents are the #1 fraud vector

When fraud attempts are broken down by type, one category leads all others — and it is not deepfakes, account takeovers, or chargebacks. It is forged and altered documents.

In 2024, forged or altered documents accounted for **50% of all fraud attempts** — more than every other category combined. The reason is structural: most onboarding and review workflows lean heavily on document verification, and the technology to forge a convincing document has never been cheaper or more accessible.

Forged documents lead every other fraud type

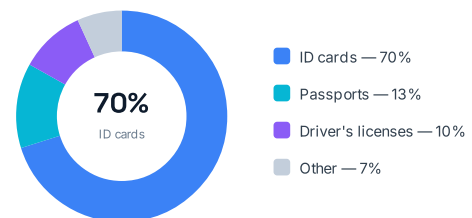
Share of fraud attempts by type, 2024



Source: Sumsb Identity Fraud Report (top fraud types, 2024)

Which identity documents get faked

Share of fraudulent identity documents



Source: Sumsb Identity Fraud Report 2025–2026

Identity fraud overall more than doubled as a share of verifications over three years — from **1.1% in 2021 to 2.6% in 2024**, easing slightly to 2.2% in 2025 as defenses improved but attacks grew more sophisticated. Two in three firms (67%) reported a year-over-year increase in fraud in 2024.

Why supporting documents are the soft target

A clean identity check does not validate the pay stub, bank statement, lease, or invoice that follows it. Those files routinely drive credit, payout, hiring, and eligibility decisions — yet identity-verification systems are not built to forensically inspect them. That gap is precisely where document fraud now concentrates.

03 The AI inflection point

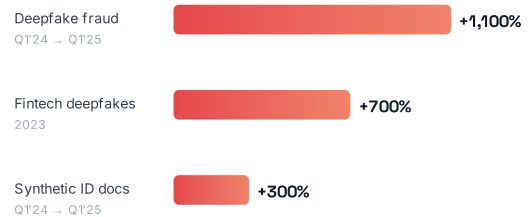
Generative AI has changed the economics of forgery. What once required skill, time, and software now requires a prompt — and the data shows attackers adopting these tools faster than any prior fraud technology.

Deepfakes reached **7% of all fraud attempts** in 2024, a fourfold increase year over year. But the sharper signal is velocity: between Q1 2024 and Q1 2025, deepfake fraud rose **1,100%** and AI-generated **synthetic identity-document** fraud rose more than 300% (311% in North America).

A genuinely new category also emerged in 2025: AI-assisted document forgery, where tools like ChatGPT, Gemini, and Grok are used to fabricate or alter documents directly. Roughly **1 in 50 forged documents** is now AI-generated — a share that did not meaningfully exist a year earlier.

AI-driven fraud is growing at unprecedented rates

Year-over-year growth (%)



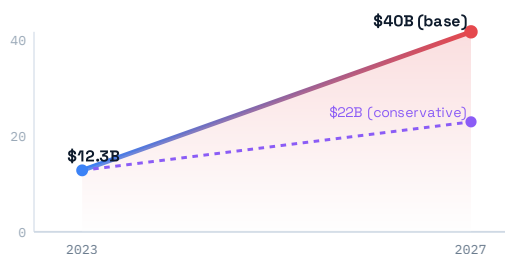
Source: Sumsb (deepfake & synthetic-doc fraud); Deloitte (fintech)

Anatomy of a modern attack — the \$25M deepfake call

In January 2024, a finance employee at engineering firm Arup joined a routine video call with the company's CFO and colleagues, and — following their instructions — wired roughly **\$25 million**. Every executive on the call was an AI-generated deepfake. The case is now treated not as an anomaly but as a template: a reusable script that attackers replicate at scale.

The projected cost of AI-enabled fraud

U.S. generative-AI fraud losses (USD billions)



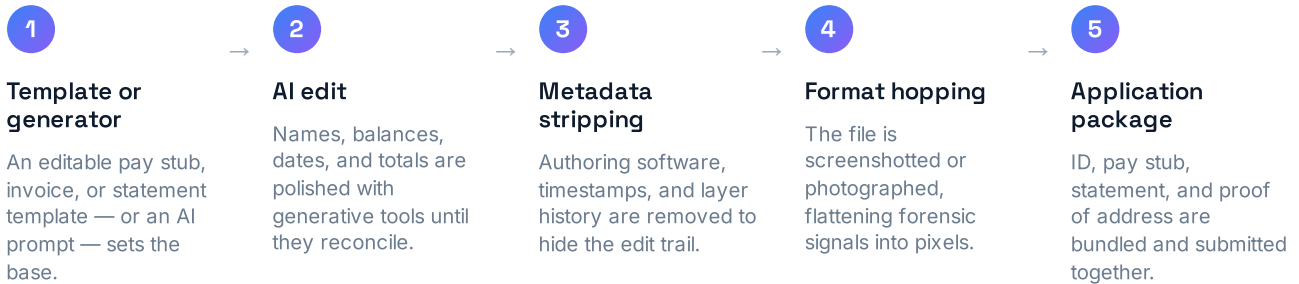
Source: Deloitte Center for Financial Services (32% CAGR, 2023–2027)

Deloitte projects that generative-AI-enabled fraud losses in the United States could more than triple — from \$12.3 billion in 2023 to **\$40 billion by 2027**, a 32% compound annual growth rate. Even the conservative scenario lands near \$22 billion.

The throughline across every dataset: the cost of producing a convincing fake is collapsing while the realism is rising. That asymmetry is what turns document fraud from a manual nuisance into an automated, industrial threat.

04 The new fraud supply chain

Modern document fraud is rarely a single edited file. It is an assembled package — built across multiple tools and formats, each step designed to add realism and erase evidence.



Format hopping erases evidence

When a native PDF becomes a screenshot or photo, the signals that prove authenticity disappear: embedded fonts, PDF object structure, creation timestamps, layer history, and source-application fingerprints. A screenshot of a bank statement isn't automatically fraud — but for income, banking, tax, and address documents, it should be treated as **elevated risk**, because the very data needed to verify it has been thrown away.

Metadata is a signal, not a verdict

A document may show traces of Adobe, Photoshop, mobile capture, or online PDF tools. Some are perfectly legitimate; some hint at manipulation. But professional fraudsters strip or normalize metadata before submission — so a clean metadata profile proves nothing on its own. Metadata earns its value only when cross-checked against structural, visual, and mathematical signals.

The danger isn't a single fake — it's the package

Older fraud changed one number in one PDF. Modern fraud assembles a coherent identity — ID, income, address, and employer — that cross-references itself. Detection therefore has to reason across an entire submission, not score one file in isolation.

05 Detection must be layered

No single signal catches modern document fraud. A clean-looking scan can hide edited numbers; perfect metadata can mask a generated file. Durable detection combines independent forensic layers into one explainable verdict.

Manual review is no longer enough

Manual fakes (2015–2022) carried visible artifacts a careful reviewer could spot. AI-assisted fakes (2024–2026) are generated and refined at scale, with plausible fonts, reconciled math, and synthetic supporting documents — then format-hopped to erase evidence and submitted across many platforms at once. Human review simply cannot scale to meet machine-speed forgery.

THE LAYERED DETECTION MODEL

01 OCR & data extraction

Read names, dates, employers, balances, and totals for downstream checks.

03 File structure

PDF objects, fonts, and layers — signs of reconstruction or editing.

05 Visual forensics

Spacing, alignment, font swaps, text replacement, image artifacts (ELA).

07 Cross-document checks

Consistency of name, address, employer, and income across a submission.

02 Math consistency

Net vs gross pay, YTD totals, statement balances, invoice arithmetic.

04 Metadata & edit trail

Authoring app and timestamps — as one signal, never a verdict.

06 AI-generation signals

Indicators of generative authoring, paired with other evidence.

08 Explainable report

Reviewer-readable evidence and reasons — not a black-box score.

Why explainability matters

A score of "87% risky" is not actionable; "the YTD total doesn't reconcile and the font changed mid-line" is. As AI fraud rises, reviewers and auditors increasingly need per-field evidence they can read, defend, and act on — which is why the final layer matters as much as the detection itself.

06 Where document fraud hurts most

The higher the volume and the faster the decision, the more attractive a workflow becomes to fraudsters. Six sectors carry the most exposure in 2026.

Lending & fintech	Manipulated income documents distort underwriting and create direct loan losses.
Tenant screening	Fake pay stubs, statements, and IDs skew approvals and shift risk onto landlords.
HR & employment	Forged work authorization, IDs, and offer letters create compliance and insider risk.
Marketplaces & gig	Template reuse scales across many onboarding accounts at near-zero cost.
Insurance claims	Fake invoices, receipts, and AI-generated evidence inflate claim leakage.
Vendor onboarding (KYB)	Fabricated business documents and bank details enable supplier and payment fraud.

07 The 2026 action checklist

- 1 Prefer original PDFs — request the native file whenever one should exist.
- 2 Treat screenshots and scans of income, ID, banking, tax, and address documents as elevated risk.
- 3 Run math checks on pay stubs, statements, invoices, and tax forms.
- 4 Combine metadata with structural, visual, and AI-generation signals — never rely on one.
- 5 Cross-check consistency of name, address, employer, and income across the whole submission.
- 6 Define risk policy before fraud happens: approve, review, request original, or decline.
- 7 Retain explainable evidence and reports for every decision, for audit and recovery.
- 8 Verify the person *and* the document — identity proofing and document forensics are two layers, not one.

Key statistics — cite this report

The numbers, at a glance

Every figure below is drawn from public reporting by the named source. Please cite the original source alongside this report.

\$12.5B	U.S. consumer fraud losses in 2024, up 25% YoY	FTC 2024
\$16.6B	Losses reported to the FBI's IC3 in 2024 (+33%); 83% cyber-enabled fraud	FBI IC3 2024
50%	of all fraud attempts in 2024 involved forged or altered documents	SUMSUB
+1,100%	growth in deepfake fraud, Q1 2024 → Q1 2025	SUMSUB
1 in 50	forged documents is now AI-generated (a 2025 first)	SUMSUB 25–26
\$40B	projected U.S. generative-AI fraud losses by 2027 (from \$12.3B in 2023)	DELOITTE

Sources & methodology

This report is a research briefing that synthesizes the most recent publicly available data from government agencies and recognized industry research. It does not rely on proprietary TrueDoc platform data; every statistic is attributable to the named third-party source below. Figures reflect reported incidents and, in the case of forward projections, modeled estimates by the cited author.

FTC — Consumer Sentinel Network Data Book 2024 (March 2025)

FBI — IC3 2024 Internet Crime Report (April 2025)

FinCEN — SAR data, via U.S. Federal Reserve Consumer Compliance Outlook (2025)

Sumsub — Identity Fraud Report (2024 and 2025–2026 editions)

Deloitte — Center for Financial Services, "Deepfake Banking Fraud Risk on the Rise" (2024)

Regula — Deepfake Trends 2024



See the evidence before you decide.

TrueDoc detects forged, tampered, and AI-generated documents — pay stubs, bank statements, IDs, invoices, screenshots, and PDFs — with layered forensic analysis and an explainable, reviewer-ready report in seconds.

Verify a document → truedoc.io