HIVE INTELLIGENCE

How Fraud Syndicates Target Banking, Insurance, and Retail in 2026 H1

What 19.7 million onboarding documents reveal about how fraud is changing in South Africa, and what it means for the teams that are tasked to prevent it.

PREPARED FOR KEY RISK & OPERATIONS LEADERS:

- Heads of Fraud & Financial Crime
- Chief Risk Officers (CROs)
- Fraud Analysts & Investigators
- Heads of Digital Onboarding
- Compliance Officers at Institutions
- Credit Risk Managers

Data Period: June 2016 to July 2026 (Focused Q1 vs Q2 2026)

www.sprinthive.com

EXECUTIVE SUMMARY

How Fraud Syndicates Are Adapting

Over the last 10 years, SprintHive has analysed 19,724,845 processed documents from 8,279,922 individuals onboarding across Retail Credit, Banking, and Insurance.

SprintHive's data shows that fraud is evolving rather than regressing over the last 6 months. The report illustrates a reduction in basic identity attacks and an increase in the sophistication of fraud attacks. This shift gives us a clear view of how fraud tactics are evolving, with deep fakes and digital replay attacks becoming increasingly sophisticated. These tactics could significantly reduce the advantage created by stronger identity controls within the next year if the rest of the industry's controls are not kept up to date.

Most notably, the data shows that document tampering increased across every major bank quarter on quarter. The tools fraudsters use to carry out these attacks also changed significantly between Q1 and Q2 2026, highlighting how quickly fraud tactics are actually evolving.

Two shifts have defined the first half of 2026. The first is a genuine increase in sophistication on the identity side. Simple presentation attacks such as holding a photo up to a camera or replaying a screen recording have fallen close to zero as fraudsters learn these no longer clear liveness checks. In their place, deep fake and digital replay attacks have climbed from a negligible share in 2024 to over 5% of identity verification attempts in Q2 2026.

The second shift is not an upgrade in sophistication, but rather a change in which tools leave edit trails. Document tampering has moved from free online PDF converters toward native editors: Microsoft Word overtook iLovePDF as the leading tool in Q2 2026, rising from 39% to 52% of tampering incidents while iLovePDF fell from 51% to 38%. Because both tools are free, mainstream, and require no special skills, the real change lies in the digital artefacts. Editing a document natively and resaving it looks more like ordinary document handling than processing a file through a converter.

From an industry perspective, SprintHive's data illustrates that retail credit providers are being targeted marginally more than banks. Within the banking sector, FNB became the most targeted bank brand on falsified statements, while Nedbank has become the fastest-growing target since the start of the year.

Who this report is for

This report is for the leaders accountable for fraud risk, customer protection and the cost of getting fraud wrong. It goes beyond reporting what is happening to explain what the data means for your decisions from setting risk thresholds and strengthening onboarding controls to briefing the board and allocating investigations capacity. Each finding is designed to help you identify emerging patterns, understand where the threat is moving, recognise where existing controls may be falling short, and determine where action is needed next.

ABOUT THIS REPORT

How we built this report

Over the last 10 years, SprintHive has been successfully embedded in the onboarding flows of retail credit, banking and insurance providers, giving a direct, high-volume view of what fraudsters actually attempt, not just what eventually gets reported as a loss.

SOURCE OF DATA

Over the last 10 years to July 2026, 19,724,845 documents were processed from 8,279,922 individuals. Every document ran through basic and advanced tamper detection. The primary focus on this report are insights over the first half of 2026 (H1)

ANALYSIS METHODOLOGY

We combined our advanced tamper detection tools to identify missed fraud: cases where documents looked clean but payment behaviour was non-existent.

THE CONSIDERATION

Not every altered document is fraud

Document tampering and fraud can overlap, but they are not the same thing. A legitimate customer may alter a document, for example, to remove password protection, without intending to commit fraud. In this case, the document has been tampered with, but no fraud has occurred.

The opposite is also true, fraud can occur without document tampering. A fraudster may use someone else's genuine, original document to commit fraud. The document itself has not been altered, but it is being used fraudulently.

First-Party Fraud

An applicant alters their own payslip or bank statement, typically changing the income amount to pass credit thresholds.

Third-Party Fraud

A fraudster changes personal details on someone else's document or uses original stolen documents outright to build a false identity.

MEASURES & COMPLIANCE

How SprintHive counters each fraud pattern

Other patterns tracked within this framework include credit profile building (also known as money muling or kite flying), where a fraudster methodically builds a false credit history over time.

1 **Advanced Document Tamper Detection** GRANULAR DETECTION

SprintHive run every document and identify specific fields that have been altered, highlighting the different fraud types rather than issue a binary pass/fail flag.

2 **Behavioural Payment-Trained Probability Models** BEHAVIOURAL AI

SprintHive models are trained on past payment behaviour and convert tampering signals into a precise fraud probability score.

3 **Identity Verification with Active Liveness** LIVENESS SHIELD

Liveness detection prevents third parties from succeeding even when presenting genuine, unaltered stolen documents.

4 **Credit Profile Building Detection Model** MULE DETECTION

The machine learning model detects money muling patterns that standard document-only checks miss.

WHY THIS MATTERS FOR COMPLIANCE AND INVESTIGATIONS

For Compliance Officers: Gives a defensible basis for distinguishing customer error from fraudulent intent when documenting customer verification decisions and maintaining an auditable record in support of FICA compliance and regulatory obligations.

For Fraud Analysts: SprintHive's tamper detection narrows investigations from "this document looks wrong" to "this specific field was changed," helping analysts prioritise genuine risk, reduce unnecessary escalations and cut case review times for their clients.

EXECUTIVE OVERVIEW

Key Findings Overview by Section

High-level executive roadmap of the 7 core analytical findings in this report

SECTION 1 **Targeted Bank Institutions** — FNB 39.63% • Standard Bank +4.28% Spike

FNB became the most frequently targeted for manipulation over the last 6 months. Standard Bank tampered statements spiked from 13.72% to 18%, and Nedbank grew from 5.75% to 9.33%.

SECTION 2 **Targeted Industries** — Retail Credit 9.9% vs Banking 7.7%

Retail Credit Providers are at a 2.2% higher risk to tampering than Banking industries.

SECTION 3 **Document Tampering Tools Shift** — MS Word 52.29% Overtakes iLovePDF 38.1%

Microsoft Word overtook PDF editors as the preferred tampering tool in Q2 2026.

SECTION 4 **Speed of Detection** — 227ms Median • <1s 90th Percentile

Sub-second document screening (median latency 227ms) ensures rigorous tamper checks do not cause customer onboarding friction.

SECTION 5 **Credit Profile Building & Money Muling** — 2.3%–2.5% Settled Range (after 3.7% Peak)

The ratio of potential credit profile building to total applications appears to have declined slightly over the past six months from 3.7% in December 2025 to roughly 2.3% in June 2026.

SECTION 6 **Identity Vectors: Simple vs Sophisticated** — Deep fakes ~5.3% • Photo-of-screen <0.2%

Basic photo-of-screen attacks dropped to <0.2%, while sophisticated deep fakes and digital replay attacks climbed to ~5.3%.

SECTION 7 **Conversion & User Experience** — 98.006% First-Try Pass Rate

98% of legitimate customers pass SprintHive's identity verification on the first attempt, proving high security does not penalise acquisition conversion.

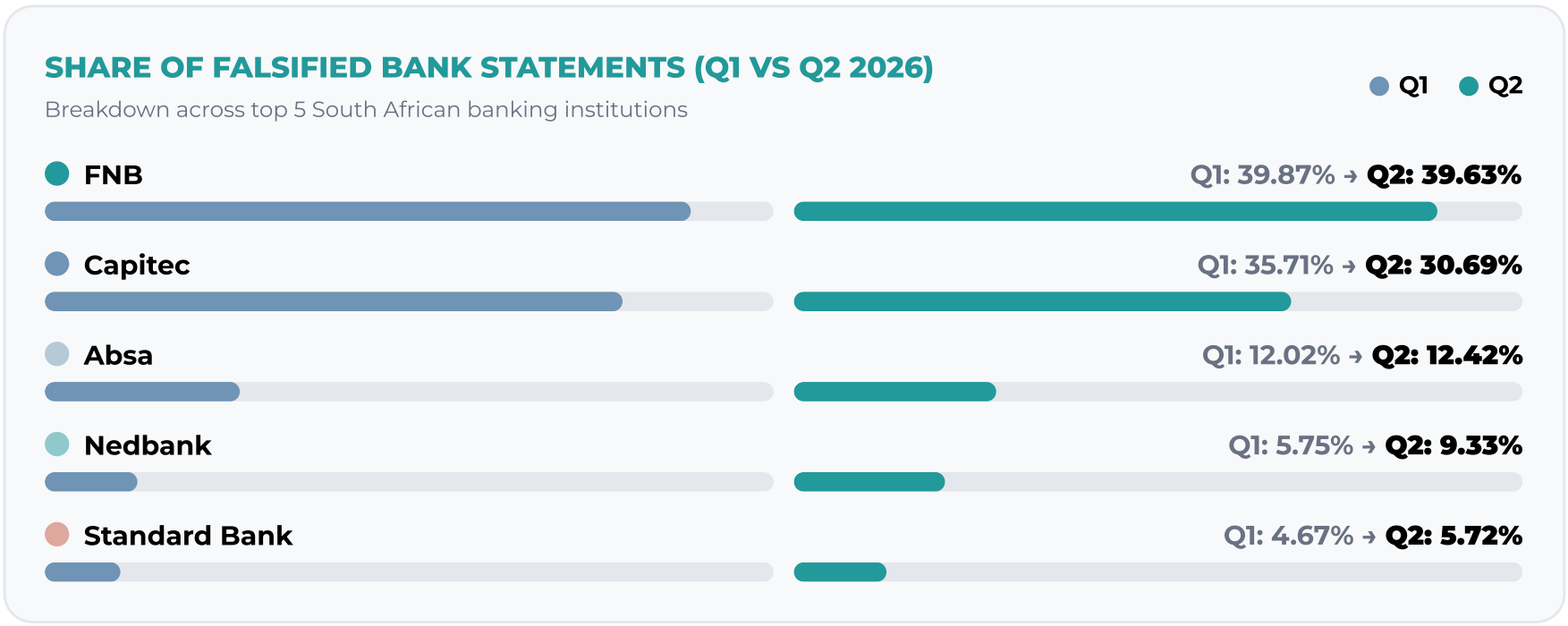
REPORT READING GUIDE

Each subsequent page details the data distributions, empirical evidence, and strategic implications for specific risk and onboarding roles.

KEY FINDINGS — SECTION 1

Which Banks Are Fraudsters Targeting?

When looking at falsified bank statements, **FNB has become the most frequently targeted brand** for manipulation in both Q1 (39.87%) and Q2 2026 (39.63%). Capitec's share fell from 35.71% to 30.69%, with a noticeable volume moving toward Nedbank (5.75% to 9.33%) and Standard Bank (4.67% to 5.72%). Absa held steady at ~12%.



Document tampering risks shifted across every major bank tracked between Q1 and Q2 2026. Standard Bank's flagged statements increased from 13.72% to 18%, while FNB rose from 15.08% to 15.89%. Discovery Bank moved in the opposite direction, declining from 29.37% to 20.85% for Warning-level flags.

DOCUMENT TAMPERING RISK ACROSS MAJOR BANKS

STANDARD BANK	FNB FLAGGED	NEDBANK VOLUME
13.72% → 18.0%	15.08% → 15.89%	5.75% → 9.33%
+4.28% Spike	High Volume	+3.58% Growth

IMPLICATION FOR RISK MANAGERS

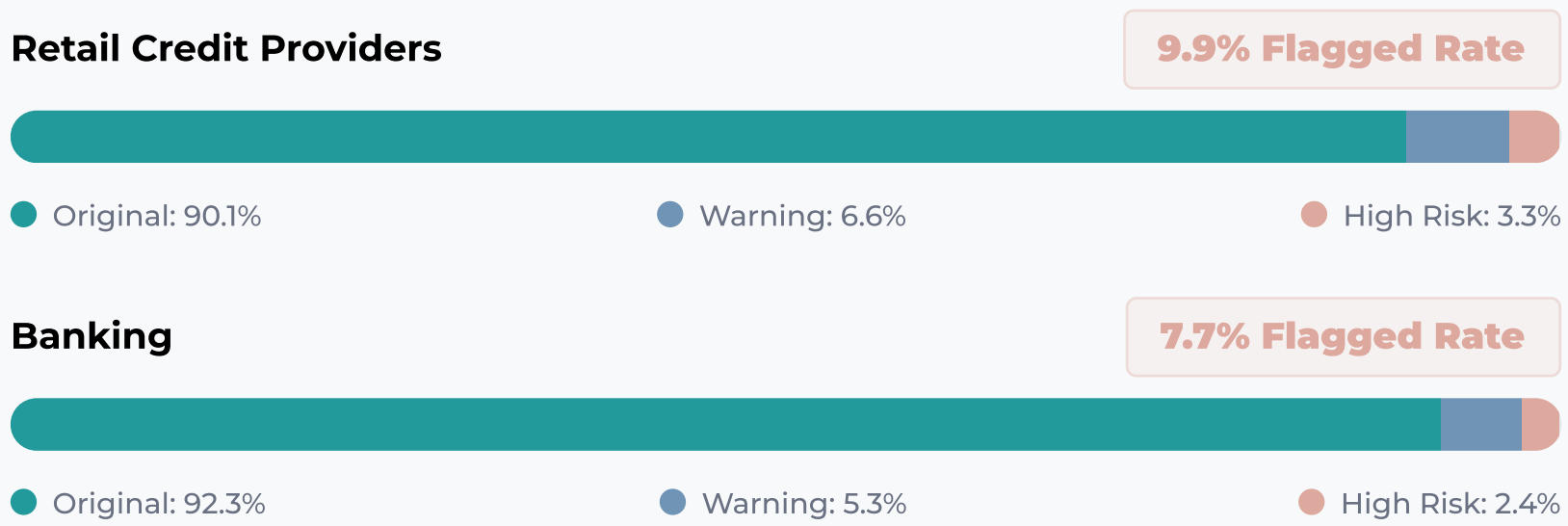
If your risk controls are calibrated to last quarter's risk profile, they may no longer reflect where manipulation is occurring today. The rising share of tampering involving Nedbank and Standard Bank statements highlights the need to continuously recalibrate risk thresholds and monitoring rules across institutions, not simply concentrate scrutiny on historically targeted banks such as FNB and Capitec.

KEY FINDINGS — SECTION 2

Which Industries Are Fraudsters Targeting?

So far in 2026, Retail Credit Providers have experienced a higher rate of document tampering than Banking. Overall, 9.9% of Retail Credit documents carried either a Warning or High Risk signal, compared with 7.7% for Banking. For Retail Credit, 6.6% were classified as Warning and 3.3% as High Risk, compared with 5.3% and 2.4%, respectively, for Banking.

FIGURE 3: DOCUMENT TAMPERING RATE BY INDUSTRY (2026 YEAR-TO-DATE)



IMPLICATION FOR ACQUISITION & ONBOARDING LEADERS

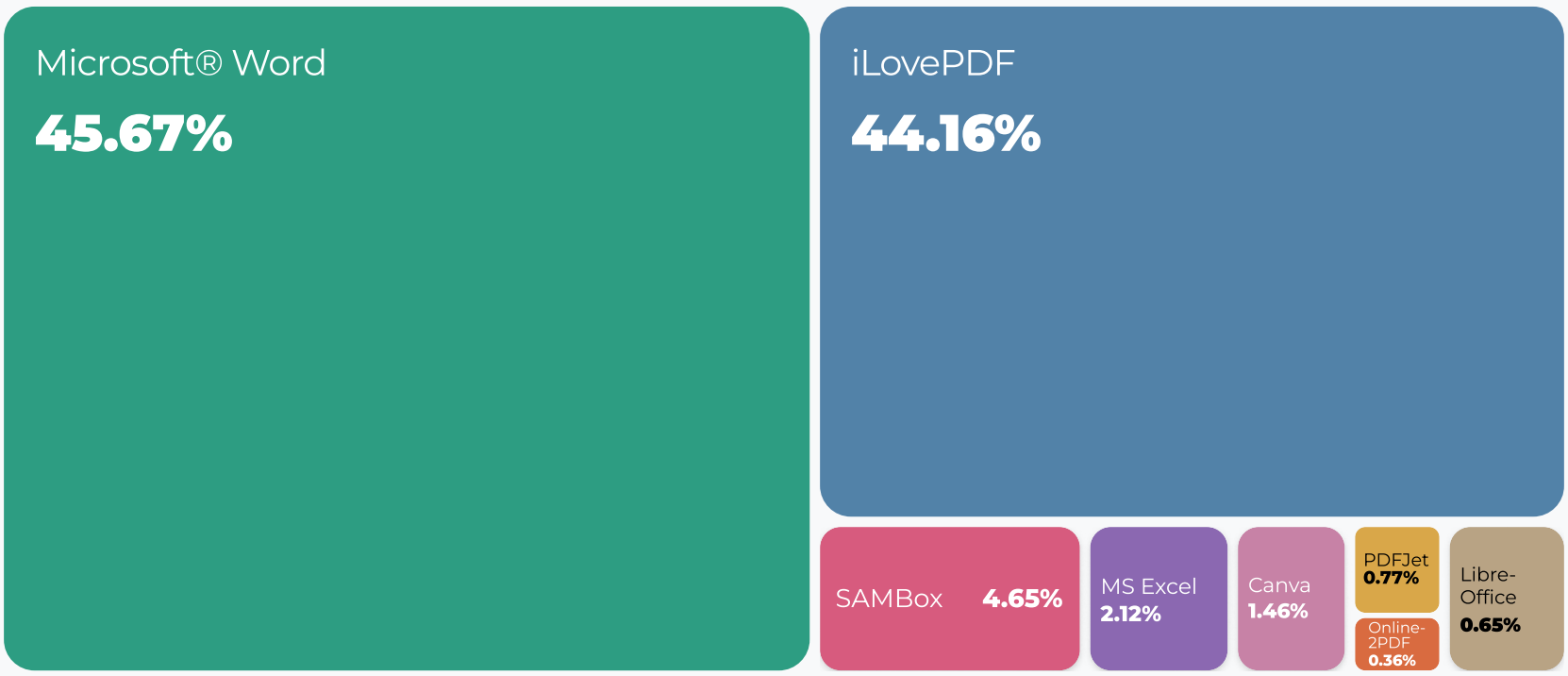
A 9.9% flagged rate in Retail Credit means that reducing verification friction to improve application conversion can carry a materially higher fraud risk in this sector than in Banking. The priority is not simply to add more checks, but to optimise your customer onboarding journey so that legitimate customers move through quickly while higher-risk applications receive proportionate scrutiny.

KEY FINDINGS — SECTION 3

The tools fraudsters use to tamper documents

Across the full analysis period, two tools account for roughly 90% of basic document tampering: **Microsoft Word (45.67%)** and **iLovePDF (44.16%)**. SAMBox (4.65%), Microsoft Excel (2.12%), Canva (1.46%), PDFjet (0.77%), LibreOffice (0.65%) and Online2PDF (0.36%) made up the remainder.

DOCUMENT TAMPERING TOOLS (12-MONTH VIEW)



The quarter on quarter shift is the more actionable signal. In Q1 2026, **iLovePDF led at 50.99%** versus Word's 39.3%. By Q2 2026, **Microsoft Word had overtaken it, 52.29%** versus iLovePDF's 38.1%.

DOCUMENT TAMPERING TOOLS (Q1 VS Q2 2026 SHIFT)

Q1 2026 LEADER	Q2 2026 SHIFT (#1)
iLovePDF (50.99%)	**MS Word (52.29%)**
MS Word: 39.3%	iLovePDF: 38.1%

IMPLICATION FOR FRAUD INVESTIGATORS

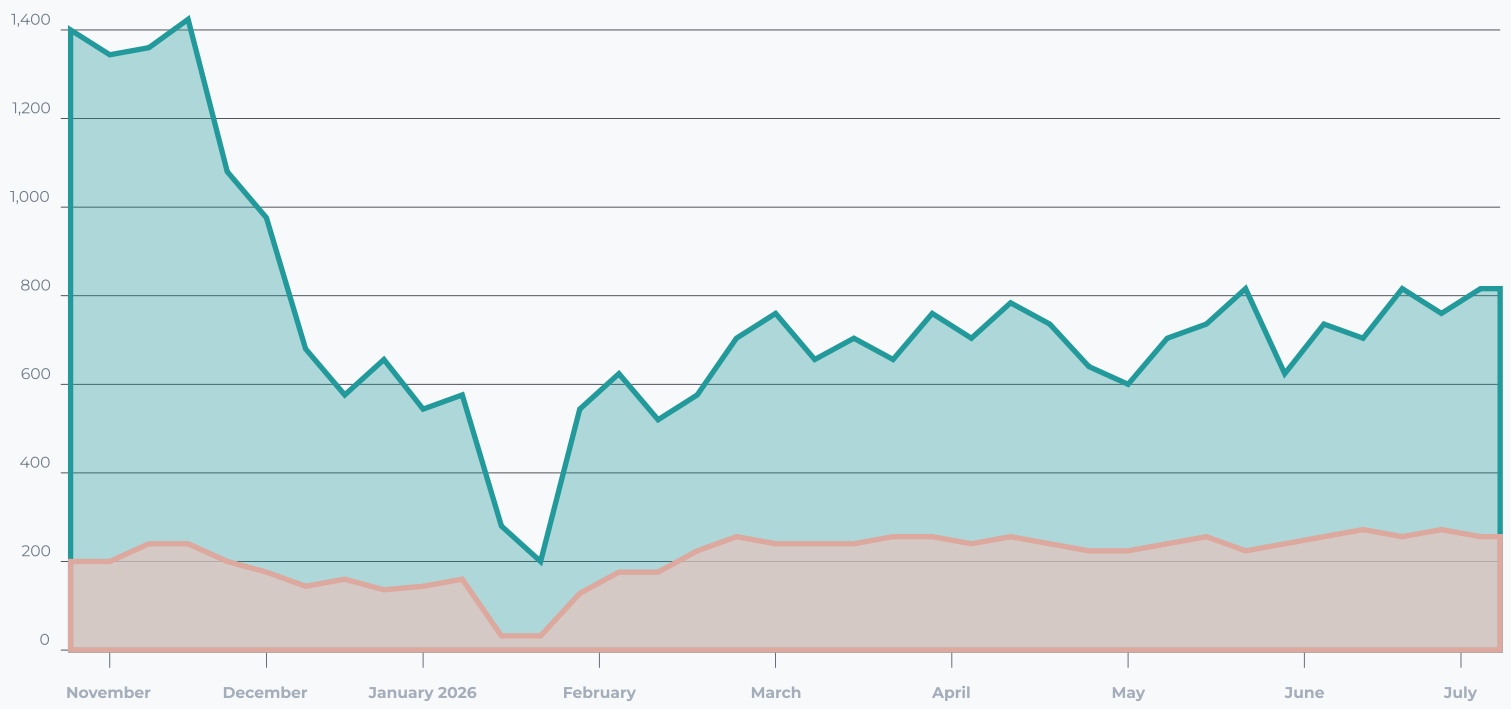
Tampering indicators vary by editing tool. A detection model tuned primarily to PDF-editor artefacts may be less effective against Word-native tampering, which became the dominant tool-based pattern in Q2. Your tools driving tamper detection should therefore be monitored and reviewed quarterly to ensure detection controls remain aligned with evolving fraud tactics.

KEY FINDINGS — SECTION 4

4. SprintHive's Speed of Fraud Detection

SprintHive's fraud detection speed has remained consistent even as application volumes and tampering complexity increased, ensuring fraudulent documents to be identified at the same speed as legitimate customers are verified. The average document check takes a twentieth of a second, and the slowest 10% of cases still complete in under one second.

AVERAGE DOCUMENT PROCESSING TIME (AUG 2025 TO JUL 2026)



227 ms

MEDIAN PROCESSING LATENCY (50TH PERCENTILE)

1/20th of a second average check speed

948 ms

TAIL CASES LATENCY (90TH PERCENTILE)

Slowest 10% of cases remain under 1 second

IMPLICATION FOR HEADS OF DIGITAL ONBOARDING

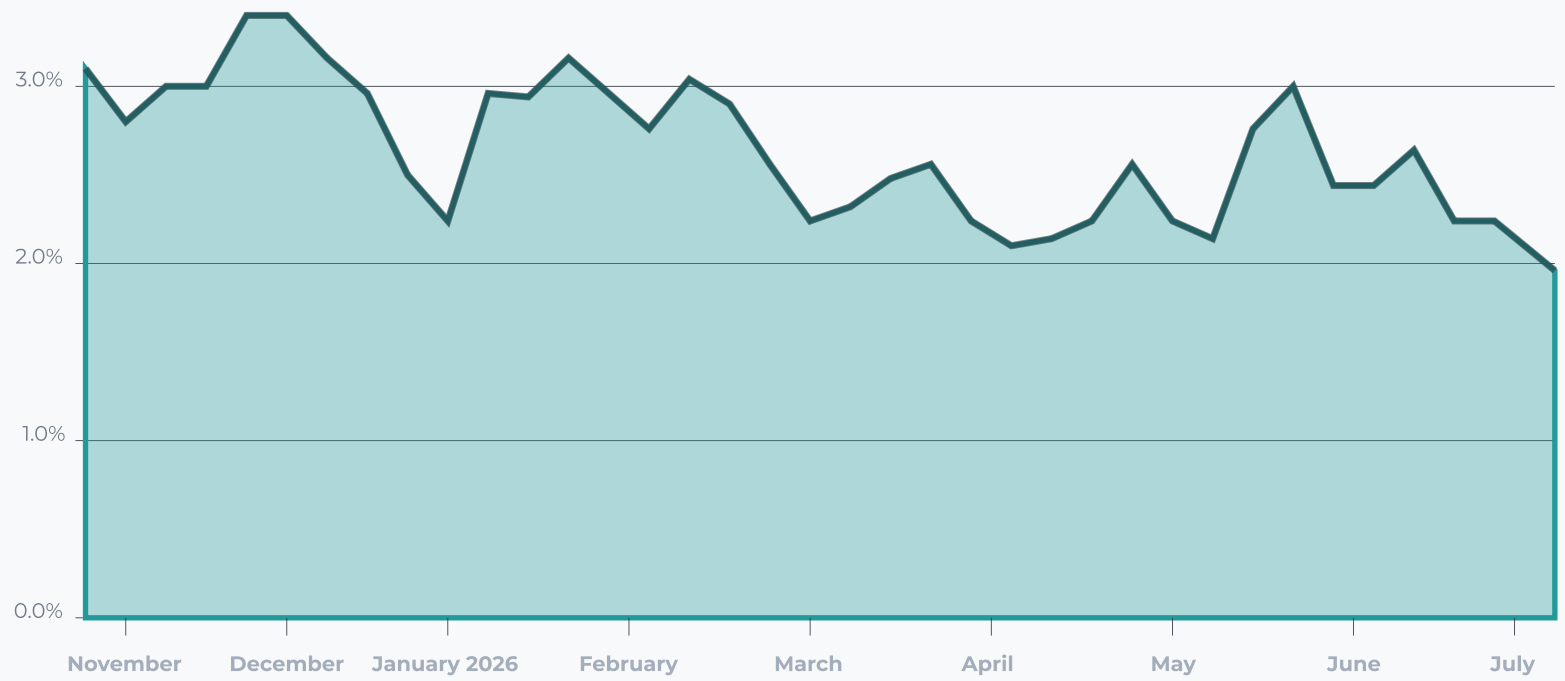
Sub-second detection means rigorous document screening does not have to come at the expense of onboarding speed. Where tamper detection operates at this speed, it should not be a bottleneck in the customer journey, allowing teams to strengthen fraud controls without adding friction for legitimate customers and letting agents review moderate and high risk cases.

KEY FINDINGS — SECTION 5

5. Credit profile building (money muling or kite flying)

The ratio of applications showing potential credit profile building against total applications peaked around **3.7% in December 2025** and has trended down since, settling at a roughly **2.3% range** by June 2026.

POTENTIAL CREDIT PROFILE BUILDING
SHARE OF TOTAL APPLICATIONS



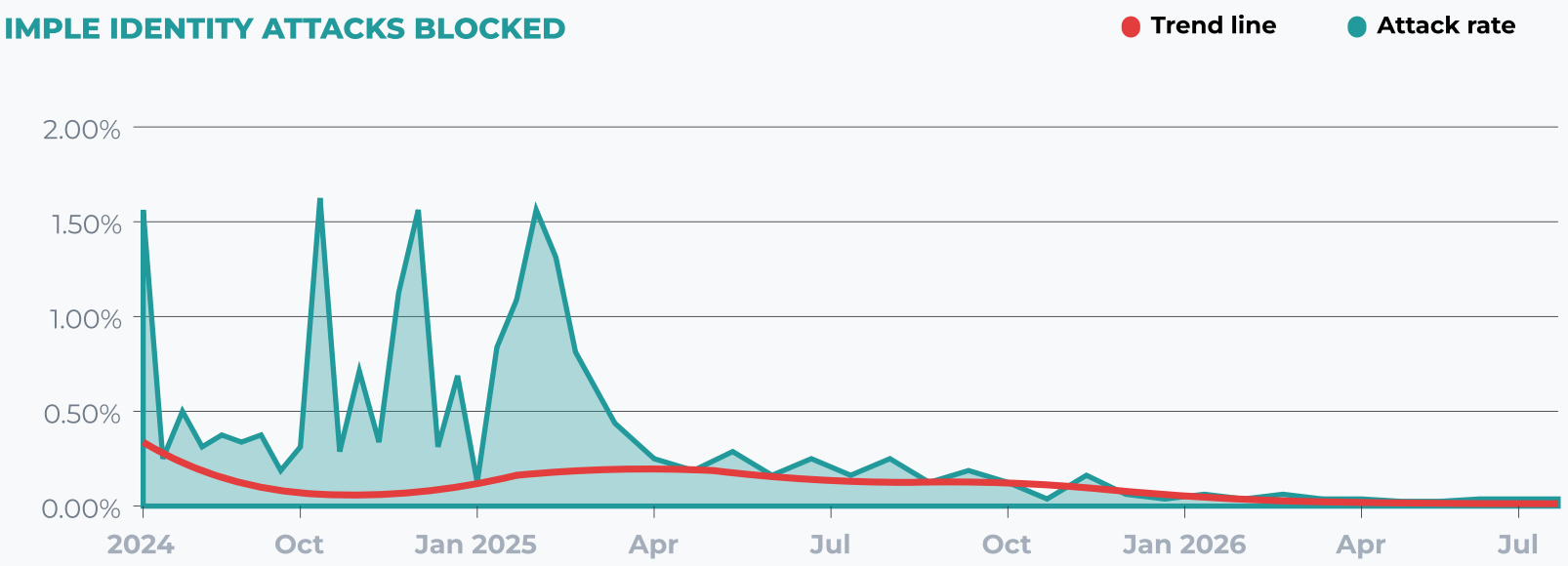
IMPLICATION FOR CREDIT RISK MANAGERS

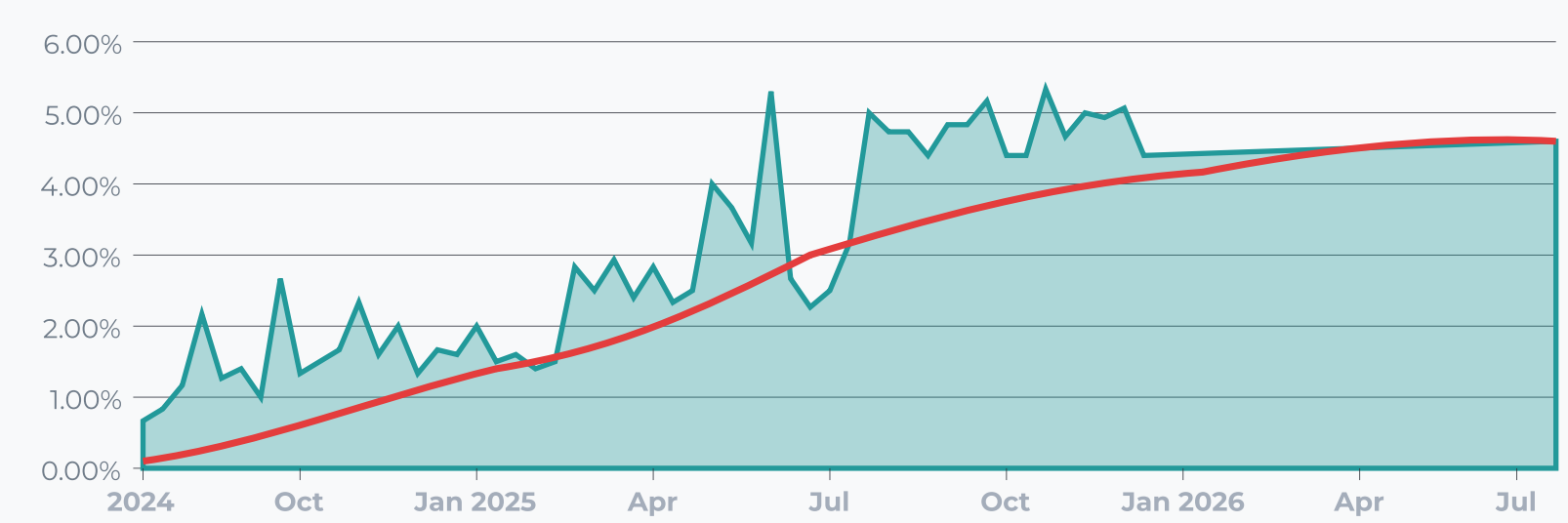
The slight decline in the ratio of potential credit profile building to total applications does not, on its own, indicate a need for tighter controls. Maintaining the current control environment is therefore appropriate, with the consideration that the December spike is worth investigating where similar seasonal application patterns may exist.

KEY FINDINGS — SECTION 6

Identity fraud is shifting from simple to sophisticated

Simple identity attacks (photo-of-screen) peaked near 1.7% in late 2024 and **fell to under 0.2% by mid-2026**. In their place, **deep fakes and digital replay** rose from ~0% in mid-2024 to **roughly 4.5% of verification attempts** by mid-2026.





STRATEGIC SIGNAL FOR CREDIT RISK OFFICER'S & FRAUD HEADS

This suggests that maintaining controls against basic presentation attacks is certainly no longer enough. Your greater investment priority should be detecting sophisticated attacks that can bypass conventional liveness checks. The sustained growth in deep fake and replay attempts over the past two years indicates that fraud strategies, detection capabilities and investment priorities need to evolve with the threat and not remain weighted towards attack methods that are already declining.

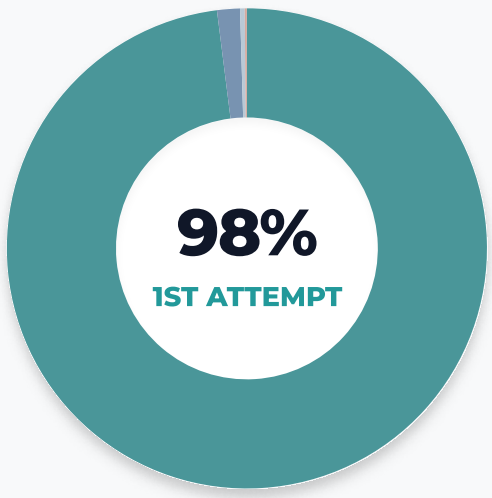
KEY FINDINGS — SECTION 7

Security has not cost SprintHive's clients conversion

98% of legitimate customers complete identity verification on the first attempt (98.006%). A further 1.537% succeed on a second attempt, 0.312% on a third, and only 0.145% need more than three attempts.

FIGURE 10: IDENTITY VERIFICATION COMPLETION ATTEMPTS PIE CHART

98.006% First Try Pass



1st Attempt	98.006%
2nd Attempt	1.537%
3rd Attempt	0.312%
> 3 Attempts	0.145%

Concerns that rigorous liveness verification and multi-point document tamper checks will increase customer drop-off are not supported by empirical evidence from our 6 million processed documents.

IMPLICATION FOR DIGITAL ONBOARDING HEADS

A 98% first-attempt completion rate is the evidence to bring into any internal debate about whether stronger verification will increase application abandonment rate.

ACTION MATRIX & TEAM RECOMMENDATIONS

Putting This To Work

Key takeaways and concrete action items tailored by institutional role.

ROLE	MOST RELEVANT FINDING	SUGGESTED ACTION ITEM
Heads of Fraud	Sophisticated attacks up ~4.5%; simple attacks down to <0.2%	**Rebalance investment from basic liveness toward deepfake and replay defence.**
CROs	Tampering rose across every major bank, Q1 to Q2 2026	**Treat per-bank and per-tool risk as a quarterly reporting line, not an annual one.**
Analysts & Investigators	Word overtook iLovePDF as leading tampering tool in Q2 (52.29% vs 38.1%)	**Review detection coverage for Word-native tampering signatures vs PDF editors.**
Onboarding & Acquisition	98% first-try IDV completion; sub-second document checks (227ms median)	**Use this data to defend verification rigour in conversion-rate discussions.**
Compliance Officers	Clear first-party vs third-party fraud framework, field-level detection	**Adopt the framework to document fraud-vs-error decisions defensibly for regulators.**
Credit Risk Managers	Credit profile building settled down to 2.3%–2.5% after a 3.7% December peak	**Hold current controls, revisit if a similar seasonal intake spike is expected.**

Implementation Tip: Share these role-specific insights with your executive steering committee to align Risk, Compliance, Product, and Engineering on 2026/7 fraud budget priorities.

COMPANY OVERVIEW

About SprintHive

A single unified platform for identity verification, income & affordability verification, and onboarding fraud prevention.

SprintHive

Protected by the Hive

Eliminate identity fraud, income misrepresentation, and document tampering during customer onboarding with SprintHive's identity verification, income and affordability verification, and onboarding fraud prevention.

CORE PLATFORM PILLARS

Identity Verification (IDV)

Automated extraction, tamper detection, and facial biometrics with passive liveness validation.

Income & Affordability Verification

Bank statement parsing, salary verification, and risk-adjusted credit profiling in real time.

Onboarding Fraud

Identify altered, forged, or manipulated documents in seconds.

Discuss what this data means for your onboarding journey

Contact your SprintHive expert sales@sprinthive.com or book a demo

Book a Demo

www.sprinthive.com

