



Fraud vs. Friction

Cross-Industry Identity Threat Index Report (2026)

Attacks or typos? Analyzing flagged ID verification sessions across industries using iDenfy's KYC software

Flagged session · **Crypto**

Verification flags

Duplicate ID face

FRAUD

Duplicate personal data

FRAUD

Underage user

FRICTION

Surname mismatch

FRICTION

Route: **Block & review**

Open case

Share of all flags raised

Fraud vs. friction

Crypto

69% fraud



Fintech

50% fraud



E-commerce

13% fraud



■ Fraud ■ Friction

METHODOLOGY

The index used real flagged sessions based on iDenfy's internal data

Every figure in this report comes from anonymized identity verification (IDV) sessions that iDenfy's platform flagged as suspicious between the period of **27 May and 26 August 2026**. Each flag carries a KYC reason code, and every reason code belongs to one of two categories. That split is the core of this index that's analyzed.

1 Fraud (intentional signals)

Duplicate faces and documents, duplicate personal data, printed or screen-captured documents, virtual cameras, AML suspicion and blacklist hits.

2 Friction (data mismatches)

Name, surname and date-of-birth mismatches, age checks, registry data mismatches, unsupported proof-of-address documents and missing additional steps.

79,764

Flagged sessions

Across 5 core industries and 12 sub-verticals

45%

Of all flags are fraud

47,854 of 106,833 flags raised

51%

Of flagged volume is iGaming

40,855 sessions, the largest single sector

69%

Fraud share in Crypto

The highest of the five core industries

87%

Friction share in E-commerce

Most flags are data-entry mismatches

1–91%

Fraud share range

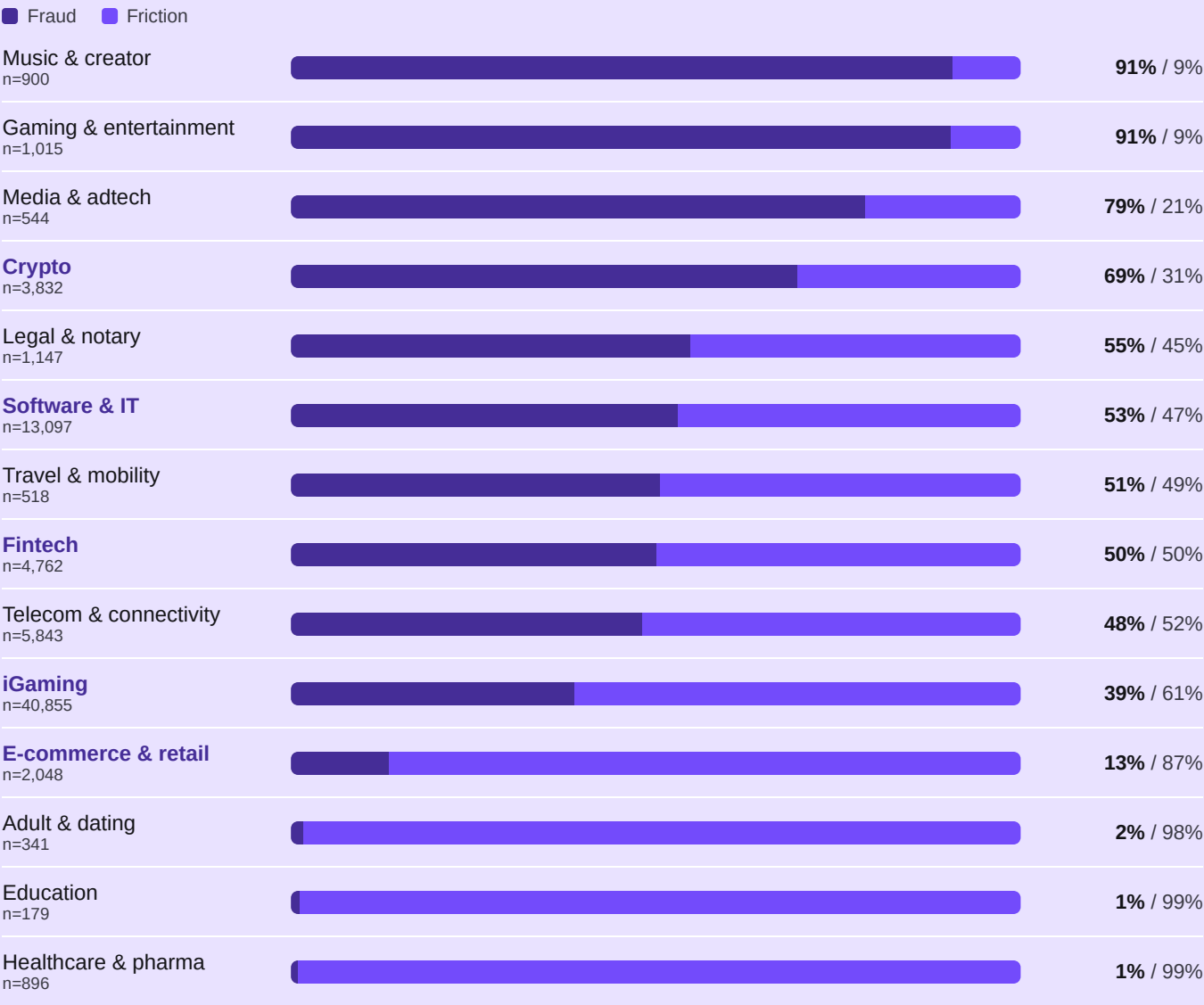
From Healthcare to Music & creator platforms

HOW TO ASSESS THE KYC STATISTICS

One user's verification can carry more than one reason code. To get the friction percentage, our team counted every flag raised in an industry, then divided the number of friction flags by that total. In E-commerce, for example, **2,406 of the 2,775 flags were friction, which gives 87%**. Fraud vs. friction splits are calculated on total flag volume. Verticals with fewer than 150 flagged sessions, plus unclassified traffic, are left out of the index view.

The same KYC flag can have a different outcome

Share of flags that are fraud vs. friction, showing how much of the flagged activity is linked to suspected fraud vs. normal data-entry problems in each industry.



ASSESSING THE KEY FINDINGS

Fraud share spans roughly 90 points, from **1% in Healthcare & pharma** to **91% on Music & creator platforms**. The top three verticals share one attack pattern: duplicate identities. On creator platforms, 74% of flagged sessions show a duplicate face. At the other end, Adult & dating flags are almost entirely age-related (87% "age not determinable"), and Healthcare flags are name and surname mismatches. One verification policy can't be right for both ends of this chart.

Two high-risk sectors compared

Crypto · 69% fraud (n=3,832)

Top reasons, share of flagged sessions

Duplicate ID face	FRAUD		33% 1,263
Duplicate face	FRAUD		22% 859
Underage user	FRICTION		21% 823
Duplicate personal data	FRAUD		13% 498
AML suspicion	FRAUD		12% 454
Age not determinable	FRICTION		11% 428
Virtual camera	FRAUD		4% 153

Duplicate faces and document duplicates lead the list. **More than 1 in 5 flagged Crypto sessions is an underage attempt**, vs. under 1% in iGaming and E-commerce. Underage is often viewed as friction, but here, due to industry specifics, it acts as a risk signal. Virtual-camera flags (4%) are also the highest of any industry analyzed in this report.

iGaming · 39% fraud (n=40,855)

Top reasons, share of flagged sessions

Duplicate ID face	FRAUD		27% 11,110
Surname mismatch	FRICTION		23% 9,443
Duplicate face	FRAUD		21% 8,707
First name mismatch	FRICTION		20% 8,182
Registry data mismatch	FRICTION		10% 3,914
Date of birth mismatch	FRICTION		7% 3,061
Personal code mismatch	FRICTION		7% 2,654

Duplicate-face signals appear 48.5 times per 100 flagged sessions, a pattern consistent with bonus abuse. Yet name and surname mismatches add another 43.1. Registry data mismatches (10%) barely appear in any other core industry. Blocking every flag here would hit genuine players as hard as multi-accounters.

55.4

Duplicate-face flags per 100

Flagged Crypto sessions, the highest of any core industry

31x

Higher underage rate

In Crypto (21%) than in iGaming (under 1%)

10.7x

More flagged sessions

In iGaming (40,855) than in Crypto (3,832)

CUSTOMER STORY

iDenfy × CSGOWIN

Beating multi-accounting and underage signups in crypto & iGaming

CSGOWin, a CS2 skin gambling platform spanning iGaming, crypto and digital assets, faced the two signals that dominate this page: **bonus-abuse rings creating duplicate accounts** and **a young audience that needed age checks before registration**.

90%+

KYC pass rate for legitimate signups

<60 sec

Average ID verification time

30%

Lower KYC/AML compliance costs

20+ hrs

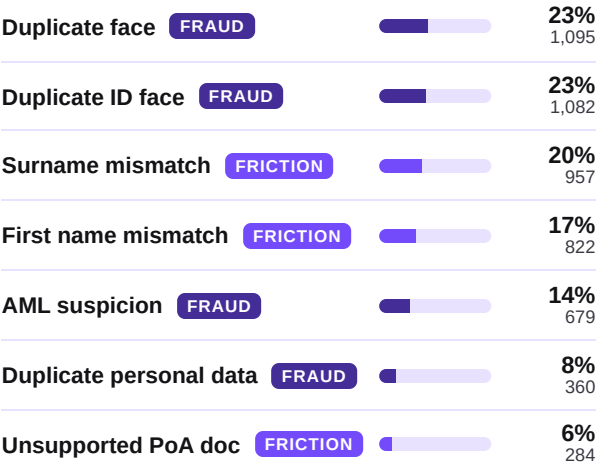
Manual review saved every week

[Read the case study →](#)

Fintech vs. e-commerce risk signal analysis

Fintech · 50% fraud (n=4,762)

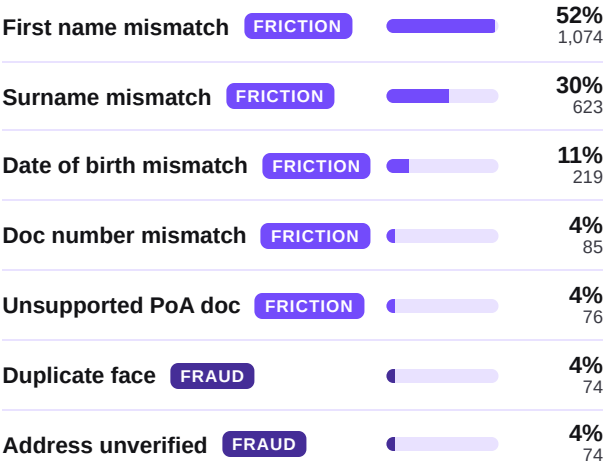
Top reasons, share of flagged sessions



Fraud and friction split almost exactly 50/50. AML suspicion appears on 14% of flagged sessions, the highest of any core industry (Crypto 12%, iGaming 1%).

E-commerce · 13% fraud (n=2,048)

Top reasons, share of flagged sessions



First name mismatches alone appear on 52% of flagged sessions. No fraud reason goes above 4%. Tightening security here adds review queues and abandoned checkouts, not protection.

All key industries analyzed side by side

INDUSTRY	FRAUD SHARE	DUPLICATE-FACE FLAGS*	NAME/SURNAME FLAGS*	AML SUSPICION	UNDERAGE
Crypto	69%	55.4	7.9	12%	21%
Fintech	50%	45.7	37.4	14%	2%
iGaming	39%	48.5	43.1	1%	<1%
E-commerce	13%	7	82.9	2%	<1%

*Per 100 flagged sessions (a session can carry both codes). Software & IT, the fifth core industry (n=13,097), sits at 53% fraud and is shown in the index.

Five ways to match verification depth to the real threat

Uniform rules either over-block low-risk users or under-protect high-risk flows. The data points to a sector-specific playbook.

01 Set rules by sector, not by default

With fraud shares running from 1% to 91%, a single company-wide threshold is guaranteed to be wrong for most verticals. Start from the index position of each product line.

02 Crypto & creator platforms: make duplicate detection a hard gate

Duplicate face and document-face matches drive most fraud here. Treat them as blocking signals, check age early in the flow, and keep liveness and virtual-camera detection on for every session.

03 iGaming: separate multi-accounting from typos

Route duplicate-face hits to block or review. Send name, surname and registry mismatches to a guided resubmission path, so genuine players aren't treated like bonus abusers.

04 E-commerce & healthcare: fix the form before the fraud stack

Where name mismatches dominate, tolerant name matching (diacritics, middle names, transliteration) and document-data prefill remove most flags without lowering security.

05 Fintech: run both playbooks in one flow

A 50/50 split plus the highest AML suspicion rate means duplicate detection, AML screening and friction-reducing matching all need to live in the same verification journey.

REGULATORY CONTEXT

Crypto-asset service providers now sit inside the EU AML perimeter, and the EU AML Regulation (AMLR) applies from July 2027. For Crypto and Fintech, detecting duplicate and synthetic identities is becoming an audit question, not just a loss-prevention one.



Turn this index into your custom verification flow

iDenfy's identity verification platform lets analysts set custom workflows and design specific KYC processes based on your operating industry and its specific risks. You can then use duplicate and liveness detection where fraud is common and use simple, low-friction KYC onboarding flows for low-risk users.

End-to-end ID verification platform with built-in AML and KYB tools.

16,000+

Document types supported

200+

Countries covered

99.9%

Verification success rate



★★★★★
4.9 / 5



[Explore Identity Verification →](#)