

The Vanishing Red Flag 2026

Media Brief

AI hasn't created new scams. It has industrialized the mechanisms that power them.

\$16.6B
FBI IC3 reported losses (2024)

\$12.5B
FTC reported fraud losses (2024)

+33%
YoY increase (IC3)

4.5x
AI-enabled scam profitability (Chainalysis)

WHY THIS MATTERS NOW

Fraud losses in the United States reached historic highs in 2024 across both federal reporting systems. The FBI documented **\$16.6 billion in reported losses (+33% YoY)**. The FTC recorded **\$12.5 billion in reported fraud losses (+25% YoY)**. Reported cryptocurrency-related fraud losses reached \$9.3 billion, a 66% increase.

Yet official federal reporting **does not isolate AI enablement** as a separate category. **Current reporting captures the outcome — not yet the mechanism.**

Moreover, the FTC's December 2025 report to Congress estimates that, adjusted for underreporting, **actual 2024 fraud losses reached \$195.9 billion — with \$81.5 billion lost by adults 60+**. FTC modeling suggests that federal databases may capture only a fraction of total fraud losses.

THE STRUCTURAL SHIFT

Fraud in 2026 is not just increasing. It is scaling.

AI is enabling:

- **Fluent, context-aware** scam messaging
- **Real-time 24/7** automated conversations
- **Deepfake** voice and video impersonation
- **Hyper-personalized targeting** using available data
- **Scalable, process-driven** fraud operations

This is not a new fraud category.

It is the industrialization of social engineering.

THE ATTRIBUTION GAP

Federal loss tables categorize fraud by scheme type (investment, imposter, BEC, tech support). **They do not isolate AI as an enabling layer.**

The FBI stated in May 2025 that AI-generated content has reached a level where it is **“often difficult to identify,”** meaning victims may not know AI was involved.

This creates a **measurable attribution gap** in official statistics — one that will persist until reporting frameworks are updated.

IMPLICATIONS FOR DETECTION

Traditional fraud mitigation has historically focused on **infrastructure-level signals** — domains, sender metadata, payment anomalies.

But when manipulation occurs **before technical red flags appear**, the detection challenge shifts from **infrastructure to content.**

The core shift is not frequency. It is coherence.

HEADLINE-READY DATA POINTS

— Verified. Citable. Ready for publication.

- **“Consumers reported losing over \$12.5 billion to fraud in 2024, a 25% increase over the prior year.”**
Source: FTC Press Release, March 2025
- **“The FBI’s IC3 reported \$16.6 billion in total reported losses in 2024, a 33% increase from 2023.”**
Source: FBI IC3 2024 Annual Report, April 2025
- **“Adjusted for underreporting, the FTC estimates 2024 fraud losses at \$195.9 billion, with \$81.5 billion lost by older adults.”**
Source: FTC, Protecting Older Consumers 2024-2025, December 2025
- **“AI-enabled scam typologies generated 4.5 times more revenue per operation than traditional scams.”**
Source: Chainalysis, 2026 Crypto Crime Report, January 2026
- **“Victims aged 60+ reported nearly \$4.9 billion in IC3 losses and filed the most complaints of any age group.”**
Source: FBI IC3 2024 Annual Report
- **“Only 13% of consumers are “very confident” in their ability to identify AI-generated threats.”**
Source: Mastercard, Consumer Cybersecurity Survey, 2025

About ZeroScam Research

Independent analysis of structural shifts in fraud dynamics using publicly available federal data, peer-reviewed research, and established industry reporting. No proprietary data or operational details are described in this analysis.

Media Contact
press@zeroscam.io
zeroscam.io/research