ZeroScam ™
Private by design

The Vanishing Red Flag Report 2026

How Generative AI Has Eliminated the Last Obvious Warning Signs of Fraud

Fraud has never been more expensive — and never looked more legitimate.

$16.6B	FBI IC3 reported losses (2024)
$12.5B	FTC reported fraud losses (2024)
+33%	Year-over-year increase (IC3)
4.5×	AI-enabled scam profitability vs. traditional (Chainalysis)

By ZeroScam Research
All data sourced from U.S. federal agencies, peer-reviewed research, and established industry reports. Published February 2026.

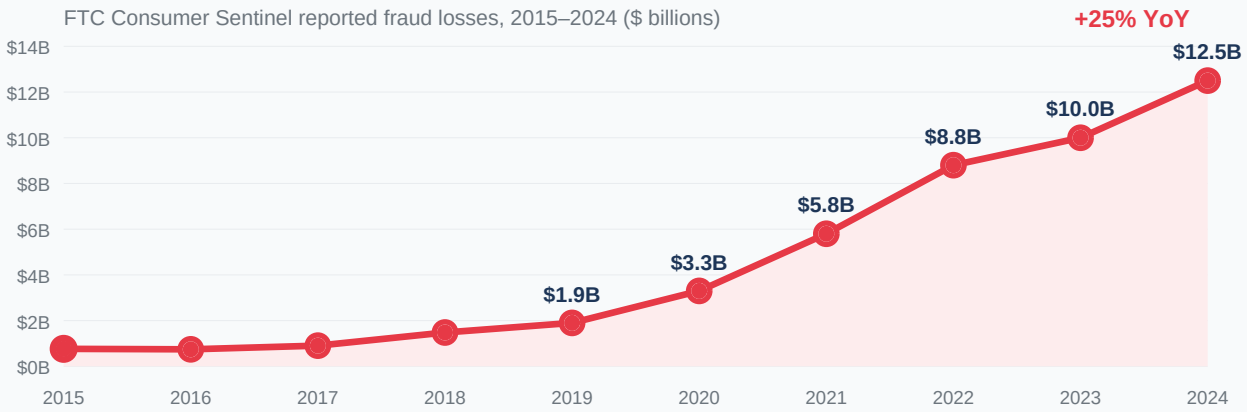
press@zeroscam.io
zeroscam.io/research

AT A GLANCE

The Scale of the Problem

U.S. Reported Fraud Losses: A Decade of Escalation

FTC Consumer Sentinel reported fraud losses, 2015–2024 ($ billions)



Source: FTC Consumer Sentinel Network Data Books, 2015–2024. See Appendix B.
2015–2016 figures use "amount paid" methodology; 2017+ use "amount lost." Not directly comparable. See Methodological Note.

FBI IC3 Reported Losses (2020–2024)

Total internet crime losses reported to IC3 ($ billions)

Source: FBI IC3 Annual Reports, 2020–2024. https://www.ic3.gov/AnnualReport/
IC3 data is voluntary and self-reported. Reporting is not mandatory; total cybercrime losses likely exceed reported figures.

"Fraud has never been more expensive — and never looked more legitimate."

— ZeroScam, The Vanishing Red Flag Report 2026

Federal-loss figures from official U.S. federal reports. Industry data from established research reports. See Appendix B for full citations.

Methodological Note — FTC Consumer Sentinel Data: Prior to 2017, the FTC reported "amount paid" by consumers in fraud complaints (values from $0 to $999,999). Beginning in 2017, the FTC shifted to reporting "amount lost," calculated only on complaints indicating losses between $1 and $999,999. As a result, figures for 2015–2016 are not directly comparable to 2017 and later years. Additionally, the FTC noted that the decrease in reported amounts between 2014 and 2015 was due primarily to the loss of a significant data contributor. Despite these methodological shifts, the overall trajectory — from under $1 billion to over $12 billion in reported losses — reflects a sustained increase in reported consumer fraud losses. FTC Consumer Sentinel figures reflect complaints received and do not represent the total universe of fraud incidents.

Methodological Note — FBI IC3 Data: The FBI notes that IC3 figures reflect complaints submitted voluntarily through ic3.gov and therefore do not represent the full scope of cybercrime activity. IC3 statistics reflect reports received through the public complaint portal and may not capture all reports made through other federal, state, or local channels. Additionally, certain loss categories — notably ransomware — exclude indirect costs such as remediation, lost productivity, and business disruption. IC3 has maintained a consistent reporting methodology across the 2020–2024 period shown in the chart, making year-over-year comparisons methodologically valid. The trajectory from $4.2 billion (2020) to $16.6 billion (2024) reflects comparable measurements.

CONTENTS

Data integrity note: *Every quantitative claim in this report is sourced from official U.S. federal agency publications (FTC, FBI/IC3), peer-reviewed academic research, or established industry reports (Chainalysis, Feedzai/GASA). No figures have been estimated, interpolated, or projected by the authors unless explicitly noted. Full citations are provided in Appendix B.*

EXECUTIVE SUMMARY

For years, consumers relied on one simple defense: bad grammar. Spelling mistakes, broken English, inconsistent formatting, and awkward phrasing acted as psychological friction that triggered analytical scrutiny.

In 2026, that friction is gone.

Generative AI has removed the last obvious red flag in scam messaging. What remains is structurally engineered persuasion: fluent, coherent, emotionally optimized, and increasingly delivered through deepfake video and cloned voice.

Meanwhile, fraud losses have reached unprecedented levels:

$12.5B FTC fraud losses (2024, +25% YoY)

FTC Consumer Sentinel, March 2025

$16.6B FBI IC3 total losses (2024, +33% YoY)

FBI IC3 Annual Report, April 2025

$9.3B Reported cryptocurrency-related fraud losses (2024, +66% YoY)

FBI IC3 Annual Report, April 2025

While reported fraud losses in the United States reached $12.5 billion (FTC Consumer Sentinel) and $16.6 billion (FBI IC3) in 2024, the FTC has acknowledged that reported complaint data does not capture the full scope of total financial harm from fraud.

In its December 2025 report to Congress, the FTC updated its underreporting analysis using 2024 data. Applying established reporting-rate assumptions (2.0% for losses under $1,000; 6.7% for losses of $1,000 or more), the agency estimated that total fraud losses for U.S. consumers of all ages in 2024 could reach $195.9 billion, with an estimated $81.5 billion attributable to adults aged 60 and over. A more conservative methodology — assuming 100% reporting for losses of $10,000 or more — yields a lower-bound estimate of $31.3 billion in total losses.

These figures are model-based estimates derived from assumed underreporting rates, not official loss tallies. The FTC notes that the scale of underreporting, particularly for high-dollar losses, "is not well understood."

Source: FTC, Protecting Older Consumers 2024–2025: A Report of the Federal Trade Commission, December 1, 2025, Section IV.A.1.g.

At the global level, survey-based estimates suggest a similarly severe landscape. The Global Anti-Scam Alliance, surveying 46,000 adults across 42 countries, estimates worldwide scam losses at $442 billion annually, with only approximately 7% of fraud victims reporting incidents (GASA, 2025).

Source: GASA & Feedzai, Global State of Scams Report 2025

While federal agencies do not yet categorize losses as AI-facilitated, multiple industry and cybersecurity reports indicate increasing use of generative AI in fraud operations.

THE ACCELERATION STACK

How Key Fraud Variables Have Shifted

The transformation of fraud is not a single change but a simultaneous shift across every operational layer. The table below summarizes how each key fraud variable has evolved between 2015 and 2026.

LAYER	2015	2026
Message quality	Broken grammar, typos	**Fluent AI-generated text**
Response time	Manual (hours/days)	**Instant AI agents (24/7)**
Voice / video presence	None or phone only	**Real-time deepfake**
Personalization	Generic ("Dear Customer")	**Data-enriched targeting**
Crypto payment rails	Emerging	**Widely adopted; $9.3B in reported cryptocurrency-related losses (IC3, 2024)**
Scale	Manual, one-at-a-time	**Thousands simultaneous**

Source: Compiled from FTC Consumer Sentinel (2015–2024), FBI IC3 (2024), Chainalysis (2026), Feedzai (2025), Mastercard (2025). See Appendix B for full citations.

The critical insight is that these layers are compounding. Each variable amplifies the others: fluent AI text makes deepfake video more believable, instant response times compress the victim's reflection window, and crypto payment rails make recovery nearly impossible. The 2015 fraud actor had to be skilled. The 2026 fraud actor only needs to be connected.

DEFINITIONS

Key Terms Used in This Report

AI-driven / AI-facilitated fraud (operational definition)

Fraud in which generative AI is used to enhance any of the following elements, regardless of scam category:

- **Message generation** — text scripts, multilingual fluency, personalization at scale
- **Impersonation media** — voice cloning, deepfake video, synthetic profile images
- **Conversation automation** — 24/7 chat agents, scaling simultaneous victims
- **Identity/KYC manipulation** — synthetic identities, document forgery assistance

AI is not treated here as a standalone scam category. Rather, it functions as an enabling layer that amplifies existing fraud types (imposters, investment, romance, BEC, tech support, etc.).

Public reporting frameworks do not currently isolate AI enablement as a distinct reporting field. Additionally, victims may not know whether synthetic media or AI-generated text was involved. This creates an **attribution gap** in official statistics, discussed in Section 8.

Additional Analytical Terms (Framework Used in This Report)

- **Persuasion architecture:** The structural design of a fraudulent communication — including authority cues, urgency framing, emotional escalation, and narrative coherence — as distinct from technical infrastructure indicators (malicious domains, IP reputation, payment rails).
- **Reaction Window:** Conceptual term used to describe the cognitive interval between emotional stimulus and analytical evaluation.
- **Emotional Velocity:** Conceptual descriptor for the speed at which a message moves a recipient from awareness to anxiety to action.

SECTION 1

The Disappearance of Surface-Level Red Flags

Historically, consumers relied on surface cues to detect fraudulent messages: misspellings, broken grammar, awkward phrasing, and formatting anomalies. These cues triggered what persuasion research describes as **central-route processing** (Petty & Cacioppo, 1986), activating analytical scrutiny that interrupted automatic compliance.

Source: Petty, R.E. & Cacioppo, J.T. (1986). The Elaboration Likelihood Model. Advances in Experimental Social Psychology, Vol. 19.

Generative AI has materially diminished these rudimentary signals by producing:

- **Highly polished scripts** across multiple languages
- **Institutional tone** consistent with legitimate business communications
- **Context-aware personalization** drawn from publicly available data
- **Fluid conversational coherence** in real-time exchanges

A Mastercard consumer survey (2025) found that only **13% of respondents were "very confident"** in their ability to identify AI-generated threats, and nearly three-quarters expressed concern that AI will make distinguishing real from fake content increasingly difficult.

Source: Mastercard, Consumer Cybersecurity Survey, 2025

The result: the message no longer looks suspicious. It looks professional. The first and most accessible defense signal has largely disappeared for the average recipient.

SECTION 2

Official Scale of U.S. Fraud Losses (2024)

Two independent federal reporting systems confirm that reported fraud losses in 2024 reached historic highs in the United States.

A. FTC Consumer Sentinel Network (2024)

- **$12.5 billion** in total reported fraud losses, a **25% increase** over 2023.
- **2.6 million** fraud reports filed; **6.5 million** total Consumer Sentinel reports.
- The percentage of consumers reporting monetary loss jumped from 27% (2023) to **38%** (2024).
- **$5.7 billion** in reported losses to investment scams alone (+24% over 2023).
- **$2.95 billion** in reported losses to imposter scams.
- Bank transfers ($2.09B) and cryptocurrency ($1.42B) were the leading payment methods.
- Fraud reporting grew from 1.2 million annual reports (2015) to 2.6 million (2024).

Source: FTC Press Release, March 10, 2025; FTC Consumer Sentinel Network Data Book 2024.

B. FBI Internet Crime Complaint Center / IC3 (2024)

- **$16.6 billion** in total reported losses, a **33% increase** from 2023.
- **859,532** complaints received; **256,256** involved actual monetary loss.
- Average loss per incident: **$19,372**.
- Cyber-enabled fraud accounted for **83% of all reported losses** ($13.7 billion).
- Top categories by reported loss: investment fraud ($6.57B), BEC ($2.77B), tech support fraud ($1.46B).

Source: FBI Press Release, April 23, 2025; IC3 2024 Internet Crime Report.

Important: *FTC and IC3 use different reporting methodologies and populations. Both reflect reported complaints and do not capture the full scope of fraud activity.*

Federal-loss figures from official U.S. federal reports. Industry data from established research reports. See Appendix B for full citations.

SECTION 3

Cryptocurrency-Related Fraud

Official Federal Data (FBI IC3, 2024)

- **$9.3 billion** in reported cryptocurrency-related fraud losses, a **66% increase** from 2023.
- **149,686** complaints involving cryptocurrency.
- Crypto investment fraud: **$5.8 billion** (41,557 complaints), +47%.
- Crypto ATM/kiosk fraud: $246.7 million (10,956 complaints), +99% in volume.
- Victims aged 60+: **$2.84 billion** in crypto-related losses alone.

Source: FBI IC3 2024 Internet Crime Report, April 2025

Industry Data (Chainalysis, January 2026)

Chainalysis estimated in its 2026 Crypto Crime Report that identified on-chain scam revenue reached at least **$14 billion in 2025**, revised upward to **$12 billion for 2024**. The firm projects the 2025 figure could exceed **$17 billion** as additional illicit addresses are identified.

- Average scam payment increased from $782 (2024) to **$2,764** (2025), a 253% increase.
- AI-enabled scam typologies generated **4.5× more revenue** per operation than traditional scams.
- Identified on-chain revenue associated with government impersonation scam typologies increased by **more than 1,400%** year-over-year.

Source: Chainalysis, 2026 Crypto Crime Report: Scams, January 13, 2026 (crypto-scams-2026 blog post) — estimates based on on-chain scam revenue and address identification.

SECTION 4

Demographic Impact & The Overconfidence Gap

- Victims **aged 60+**: nearly **$4.9 billion** in reported IC3 losses (2024), +43% YoY, most complaints of any group (147,127).
- Within crypto fraud: this group reported **$2.84 billion** in losses.
- California, Texas, and Florida ranked highest in both complaint volume and reported losses.
- Younger adults (20–29): **44% of reported fraud complaints** involved monetary loss (FTC, 2024).

Source: FBI IC3 2024; FTC Consumer Sentinel 2024; TRM Labs, April 2025

The Overconfidence Gap

A recurring finding across multiple surveys is the dangerous gap between perceived and actual scam detection ability. The GASA 2025 global survey found that **73% of respondents believed they could identify a scam**, yet **23% had lost money to one**. Mastercard's 2025 survey found that younger adults reported the highest confidence levels while also reporting the highest engagement with suspected scam attempts.

Source: GASA & Feedzai, Global State of Scams Report 2025; Mastercard, 2025

This asymmetry — **high confidence** combined with **diminished usefulness of traditional red-flag indicators** — is precisely the vulnerability that AI-polished fraud exploits. When visible errors disappear, **the illusion of control remains**.

SECTION 5

AI as a Persuasion Multiplier

Generative AI does not invent new psychological vulnerabilities. It scales existing ones.

- **Elaboration Likelihood Model** (Petty & Cacioppo, 1986): The reduction of visible credibility gaps may decrease the likelihood that recipients engage in central-route scrutiny.
- **Truth-Default Theory** (Levine, 2014): Humans assume communications are truthful until triggered otherwise. AI reduces the likelihood that typical deception triggers are activated.
- **Prospect Theory** (Kahneman & Tversky, 1979): Loss aversion makes urgency framing disproportionately effective. AI enables urgency framing to be deployed consistently and at scale.

As an analytical grouping used in this report, AI simultaneously improves three critical persuasion variables: **authority mimicry** (institutional tone, deepfaked executives), **urgency compression** (instant escalating pressure), and **emotional clarity** (fluent, error-free framing).

Case 1: The Arup Deepfake ($25.6 Million, January 2024)

In January 2024, a finance employee at Arup, a UK-based multinational engineering firm, was deceived into making **15 separate transfers totaling approximately $25.6 million** (HK$200 million) to **five distinct bank accounts** after a video conference where every attendee—including the CFO and senior executives—was an AI-generated deepfake. The employee had initially suspected fraud based on a phishing email, but the visual and auditory confirmation from the video call overrode his skepticism. Arup's CIO, Rob Greig, later characterized the incident as "technology-enhanced social engineering" rather than a conventional cyberattack.

Source: CNN Business, May 2024; World Economic Forum, February 2025; Hong Kong Police

Case 2: Hong Kong Deepfake Banking Ring ($193 Million, April 2025)

In April 2025, Hong Kong police arrested 8 suspects accused of using deepfake technology to bypass bank identity verification and open fraudulent accounts using stolen ID cards. The broader operation, conducted between April 7–17, led to 503 total arrests with losses exceeding HK$1.5 billion (US$193.2 million). The syndicate used at least 21 reported-lost Hong Kong ID cards to submit 44 bank account applications, merging the facial features of fraudsters with the appearance of cardholders via deepfake. Of 44 applications, **30 were approved**—enabling systematic money laundering and credit line exploitation. This illustrates **systematic exploitation of KYC verification processes using synthetic identity techniques**.

Source: South China Morning Post, April 19, 2025; Hong Kong Police Force

Case 3: FBI AI Voice Cloning Advisories (December 2024 – May 2025)

The FBI issued two major public service announcements within six months. In December 2024 (IC3 Alert I-120324-PSA), the FBI warned that criminals exploit generative AI to commit fraud at greater scale, increasing the credibility of their schemes. In May 2025 (IC3 Alert PSA250515), the FBI reported that since April 2025, malicious actors have sent AI-generated text and voice messages impersonating senior U.S. officials, targeting

current and former federal and state officials and their contacts. The FBI stated that AI-generated content has reached a level where authenticity is often difficult to identify. CrowdStrike separately reported a **442% increase** in voice phishing (vishing) activity between the first and second halves of 2024, attributing the surge to AI-driven phishing and impersonation tactics.

Source: FBI IC3 PSA I-120324-PSA (Dec 2024); FBI IC3 PSA250515 (May 2025); CrowdStrike 2025 Report

SECTION 6

The Shrinking Reaction Window

We introduce the concept of the **"Reaction Window"** — the cognitive interval between emotional stimulus and analytical evaluation. AI-driven scams reduce opportunities for reflective delay because:

- **Instant response times:** AI chatbots sustain real-time conversations 24/7, reducing natural pauses for reflection.
- **Immediate narrative escalation:** Scripts move from contact to urgency framing often within minutes rather than days.
- **Continuous reinforcement:** AI-generated interactions maintain persistent emotional pressure on victims—sustained urgency, repeated trust signals—without the inconsistencies introduced by human fatigue.

From an operational standpoint, AI enables attackers to conduct dozens of simultaneous fraud conversations at scale, significantly reducing the human bottleneck that previously limited social engineering campaigns.

We describe the resulting dynamic as **Emotional Velocity**: the speed at which a message moves a recipient from awareness → anxiety → action. According to the GASA Global State of Scams Report 2025, approximately **two-thirds of scams reported worldwide are concluded within a day of first contact**, suggesting that the reaction window in many scams is extremely short in practice.

Source: GASA & Feedzai, Global State of Scams Report 2025

SECTION 7

The Industrialization of AI-Driven Fraud

Fraud in 2026 is not merely increasing in volume. It is industrializing.

Across independent industry reports, a consistent pattern emerges: **AI is transforming fraud from isolated deception into scalable infrastructure.**

In a 2025 Feedzai global survey of 562 fraud and financial crime professionals, an overwhelming **92% reported observing fraudsters leveraging generative AI** in their attacks, and more than half indicated that AI is now involved in a significant portion of fraud incidents. Notably, around **60% of respondents identified deepfakes or voice cloning as a major concern**—an indication that sophisticated synthetic media are now widespread enough to shape risk perceptions and operational priorities across the financial sector.

These findings reflect not isolated cases but a broader shift in how fraud operations are conducted and perceived, with AI technologies increasingly embedded in both offensive tactics and defensive systems.

Source: Feedzai, AI Trends in Fraud and Financial Crime Prevention, May 6, 2025.

Chainalysis reports that identified AI-linked scam clusters demonstrate significantly greater operational intensity compared to non-AI clusters:

- **Higher median daily revenue:** $4,838 vs. $518
- **Increased transaction volume:** 35.1 vs. 3.89 average transfers per day (approximately 9× higher activity)

These metrics suggest higher operational efficiency and broader simultaneous victim engagement. The elevated transaction volume indicates that AI-linked operations are able to manage more interactions in parallel, consistent with a shift toward scalable, process-driven fraud infrastructure.

While these figures do not directly measure persuasion effectiveness, they indicate that AI-linked scam operations are generating greater on-chain revenue and processing substantially more transactions per day.

Source: Chainalysis, Crypto Crime Report 2026: Scams, January 2026.

This is not merely growth. It is operational scaling.

Sumsub's 2025 Annual Identity Fraud Report describes what it calls a "Sophistication Shift" in global fraud operations. Based on analysis of millions of verification checks and more than four million detected fraud attempts worldwide, the report finds that fraud is increasingly characterized by **coordinated, multi-step schemes** rather than isolated, low-effort attacks.

Instead of relying on single-point document manipulation or basic identity spoofing, attackers are combining:

- **AI-assisted document forgery**
- **Synthetic identity construction**
- **Cross-channel account manipulation**
- **Layered social engineering**

Notably, AI-assisted document forgery — virtually absent in 2024 — accounted for approximately **2% of detected fraudulent verification attempts in 2025**, reflecting measurable operational adoption of generative tools in identity fraud workflows.

The report further warns of the emergence of "agentic AI scams," in which automated systems are capable of executing multi-stage fraud processes with reduced human oversight. This marks a shift from manual deception toward process-driven, scalable fraud infrastructure.

In parallel, **75% of surveyed fraud and compliance professionals** expect fraud to become increasingly AI-driven in the near term.

Source: Sumsub, Fraud Shifts to Complex Multi-Step Schemes in 2025; Agentic AI Scams Poised to Surge in 2026, November 2025.

The pattern is consistent across telemetry, compliance datasets, and industry surveys: fraud is becoming process-driven and systematized.

Gartner predicts that by 2026, **30% of enterprises will regard standalone identity verification and authentication solutions as unreliable in isolation** due to the rising sophistication of AI-generated deepfakes.

Source: Gartner, Predicts 2026: Identity Verification Reliability, February 1, 2024.

AI-Enhanced Social Engineering

Fraud has always relied on social engineering: manipulating trust, authority, and urgency to override skepticism.

What has changed is not the tactic—but the scale and precision.

Generative AI allows attackers to transform fragments of compromised data and publicly available information into coherent, highly personalized narratives. Instead of generic phishing emails, victims now receive messages referencing real employers, recent transactions, geographic details, or professional affiliations—details that make the fraud feel plausible.

Access to personal accounts through email compromise, SIM swapping, or credential reuse enables cascading exploitation across platforms.

AI does not invent new psychological weaknesses. It industrializes them—turning what was once a craft practiced by skilled fraudsters into a scalable, automated system.

SECTION 8

What Official Data Does Not Yet Tag

As established in the Definitions section, AI is an enabling layer, not a scam category. This creates a fundamental measurement problem.

As of early 2026, neither the FTC nor the FBI/IC3 systematically isolates "AI-generated" or "AI-facilitated" as a distinct field in their published loss tables. This is not a failure of intent—it is a **material attribution gap** reflecting the nature of the problem:

- AI **amplifies existing fraud schemes** (romance, investment, impersonation, BEC) rather than creating a separate, neatly measurable category.
- Victims themselves **may not know** whether synthetic media or generated text was used. The FBI stated in its May 2025 PSA that AI-generated content has reached a level where authenticity is **"often difficult to identify."**

Despite this gap, a convergence of industry evidence points to AI's growing role. *Industry data should be interpreted as directional indicators, not official loss attribution.*

- According to a 2025 Feedzai survey of financial institutions, **92% report encountering generative AI** in fraud operations.
- Chainalysis reports that AI-enabled scam services are associated with **significantly higher revenue efficiency** compared to non-AI scam operations.
- The FBI's December 2024 PSA *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud* notes that **"since it can be difficult to identify when content is AI-generated,"** criminals are using generative AI to enhance text, images, audio, and video in fraud schemes.

Source: FBI IC3, PSA I-120324-PSA, December 3, 2024. https://www.ic3.gov/PSA/2024/PSA241203

- The IC3 2024 Annual Report noted **rising attack sophistication** across multiple fraud categories.
- The FBI's May 15, 2025 Public Service Announcement on senior U.S. official impersonations notes that **"AI-generated content has advanced to the point that it is often difficult to identify,"** and advises that when in doubt about authenticity, individuals should contact relevant security officials or the FBI for help. The advisory references vishing (voice phishing — fraudulent phone calls, including those using AI-generated or synthetic audio) and smishing (SMS phishing — deceptive text messages) as vectors exploiting AI-generated audio and text.

Source: FBI, Senior U.S. Officials Impersonated in Malicious Messaging Campaign, May 15, 2025.

The official loss figures **do not currently isolate AI enablement as a separate reporting field**. If AI-specific tagging is introduced in future reporting cycles, the measurable impact may become clearer.

SECTION 9

Why This Will Likely Escalate

1. Near-zero marginal cost.

Sophisticated phishing kits now cost less than $500 (Chainalysis). Consumer-grade voice synthesis tools can generate realistic voice clones from short audio samples. Consumer-grade tools enable anyone to generate polished audiovisual content in minutes.

Source: Chainalysis, 2026 Crypto Crime Report

2. Widespread model access.

Open-source language models, face-swap tools, and voice synthesis systems are broadly available. Chainalysis documented AI vendor services sold through Telegram, specifically marketed to fraudsters.

3. Detection gaps in the persuasion layer.

Most fraud detection focuses on infrastructure signals. When emotional manipulation occurs before any link click or malicious domain visit, infrastructure-focused detection may react too late.

Fraud actors iterate faster than consumers adapt. The evidence suggests this is not a temporary spike, but a structural shift.

SECTION 10

Implications for Fraud Detection

The core shift is not frequency. It is coherence. AI hasn't created new fraud categories. It has industrialized the mechanisms that power them — from persuasion to infrastructure.

When fraud messaging becomes increasingly difficult to distinguish from legitimate communication—especially at scale—and when that messaging is delivered through deepfaked video and cloned voices, the detection challenge fundamentally changes.

Traditional fraud mitigation focuses on:

- Malicious domain identification
- Known sender databases and URL blacklists
- Payment channel blocking
- Post-transaction anomaly detection

These remain necessary. But when persuasion occurs before any infrastructure signal is triggered, a complementary approach becomes relevant: analyzing **message architecture**—persuasion structure, urgency patterns, authority mimicry, and emotional escalation dynamics.

This is an analytical observation based on publicly available research. It is not a product promotion.

THE COST OF INACTION

What Happens If Current Growth Continues

$12.5B FTC reported fraud losses (2024)	**$16.6B** FBI IC3 total losses (2024)

$9.3B Crypto fraud losses (2024, +66% YoY)	**+43%** Increase in losses for victims aged 60+	**38%** Of fraud reporters lost money (up from 27%)

> ***"Fraud losses are at record highs. At the same time, the visible warning signs have disappeared."***
>
> **— ZeroScam, The Vanishing Red Flag Report 2026**

A simple mathematical observation:

FBI IC3 reported losses grew from $12.5 billion (2023) to $16.6 billion (2024), a 33% year-over-year increase. FTC reported losses grew from $10 billion (2023) to $12.5 billion (2024), a 25% increase. If either growth rate persists into the next reporting cycle, reported losses would exceed $20 billion.

Note: *This is a straightforward extrapolation of published year-over-year growth rates, not an official projection. Actual outcomes will depend on enforcement actions, regulatory changes, consumer awareness, and technological countermeasures. However, the structural drivers described in this report—near-zero cost AI content, widespread model access, and detection gaps—suggest that a meaningful deceleration is not the default trajectory.*

Federal-loss figures from official U.S. federal reports. Industry data from established research reports. See Appendix B for full citations.

APPENDIX A

Headline-Ready Data Points

The following are accurate, officially sourced, and suitable for direct citation in journalism.

1. "Consumers reported losing over $12.5 billion to fraud in 2024, a 25% increase over the prior year."

Source: FTC Press Release, March 10, 2025

2. "The FBI's Internet Crime Complaint Center reported $16.6 billion in total losses in 2024, a 33% increase from 2023."

Source: FBI Press Release, April 23, 2025; IC3 2024 Annual Report

3. "Cryptocurrency-related fraud accounted for $9.3 billion in reported losses in 2024, a 66% increase, across 149,686 complaints."

Source: FBI IC3 2024 Internet Crime Report

4. "Victims aged 60+ reported nearly $4.9 billion in total IC3 losses in 2024 and filed the most complaints of any age group."

Source: FBI IC3 2024; FBI Press Release, April 2025

5. "The percentage of FTC fraud reporters who lost money rose from 27% in 2023 to 38% in 2024."

Source: FTC Consumer Sentinel Network Data Book 2024

6. "AI-enabled scams generated 4.5 times more revenue per operation than traditional scams in 2025."

Source: Chainalysis, 2026 Crypto Crime Report, January 2026

7. "92% of financial institutions surveyed report that fraudsters use generative AI."

Source: Feedzai, 2025 AI Trends in Fraud and Financial Crime Prevention, May 2025

8. "Only 13% of consumers are "very confident" in their ability to identify AI-generated threats."

Source: Mastercard, Consumer Cybersecurity Survey, 2025

9. "73% of adults believe they can identify a scam, yet 23% have lost money to one."

Source: GASA & Feedzai, Global State of Scams Report 2025

APPENDIX B

Full Source References

Federal Agency Reports

[1] Federal Trade Commission. "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024." March 10, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[2] Federal Trade Commission. Consumer Sentinel Network Data Book 2024. March 2025. ftc.gov/reports/consumer-sentinel-network-data-book-2024

[3] Federal Trade Commission. Consumer Sentinel Network Reports (all years). https://www.ftc.gov/enforcement/consumer-sentinel-network/reports

[4] Federal Bureau of Investigation. "FBI Releases Annual Internet Crime Report." April 23, 2025. fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

[5] FBI Internet Crime Complaint Center (IC3). 2024 Internet Crime Report. April 2025. ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[6] FBI Internet Crime Complaint Center (IC3). Annual Reports (all years, 2014–2024). https://www.ic3.gov/AnnualReport/

[7] Federal Trade Commission. "Protecting Older Adults from Fraud." Report to Congress, October 2024. https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf

Industry Research Reports

Industry surveys and commercial research reports are cited as directional indicators of AI adoption in fraud, not as official loss attribution.

[8] Chainalysis. 2026 Crypto Crime Report: Scams Chapter. January 13, 2026. https://www.chainalysis.com/blog/crypto-scams-2026/

[9] Feedzai. "2025 AI Trends in Fraud and Financial Crime Prevention." May 6, 2025. https://www.feedzai.com/pressrelease/ai-fraud-trends-2025

[10] GASA & Feedzai. "Global State of Scams Report 2025." November 2025. https://www.feedzai.com/resource/global-state-of-scams-report-2025/

[11] Sumsub. "Fraud Shifts to Complex Multi-Step Schemes in 2025; Agentic AI Scams Poised to Surge in 2026." November 2025. https://sumsub.com/newsroom/sumsubs-annual-report-fraud-shifts-to-complex-multi-step-schemes-in-2025-agentic-ai-scams-poised-to-surge-in-2026/

[12] Mastercard. "Consumer Cybersecurity Survey 2025." 2025. https://www.mastercard.com/global/en/news-and-trends/stories/2025/consumer-cybersecurity-survey.html

[13] TRM Labs. "A Record-Breaking Year for Cybercrime: Key Findings from the FBI's 2024 IC3 Report." April 2025. https://www.trmlabs.com/resources/blog/a-record-breaking-year-for-cybercrime-key-findings-from-the-fbis-2024-ic3-report

[14] Gartner. "Gartner Predicts 30% of Enterprises Will Consider Identity Verification and Authentication Solutions Unreliable in Isolation Due to AI-Generated Deepfakes by 2026." February 1, 2024. https://www.gartner.com/en/newsroom/press-releases/2024-02-01-gartner-predicts-30-percent-of-enterprises-will-consider-identity-verification-and-authentication-solutions-unreliable-in-isolation-due-to-deepfakes-by-2026

Academic & Institutional References

[15] Petty, R.E. & Cacioppo, J.T. (1986). "The Elaboration Likelihood Model of Persuasion." Advances in Experimental Social Psychology, Vol. 19, pp. 123–205.

[16] Chaiken, S. (1980). "Heuristic versus systematic information processing." J. Personality and Social Psychology, 39(5), pp. 752–766.

[17] Levine, T.R. (2014). "Truth-Default Theory (TDT)." J. Language and Social Psychology, 33(4), pp. 378–392.

[18] Kahneman, D. & Tversky, A. (1979). "Prospect Theory." Econometrica, 47(2), pp. 263–291.

[19] World Economic Forum. "Cybercrime: Lessons from a $25m deepfake attack." February 2025. https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

[20] CNN Business. "Arup revealed as victim of $25 million deepfake scam." May 17, 2024. https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

[21] Lyu, S. (Univ. at Buffalo). "2026 will be the year you get fooled by a deepfake." Fortune, Dec 27, 2025. https://fortune.com/2025/12/27/2026-deepfakes-outlook-forecast/

[22] South China Morning Post. "Hong Kong police arrest 8 over deepfake scams bypassing bank security checks." April 19, 2025. https://www.scmp.com/news/hong-kong/law-and-crime/article/3307159/hong-kong-police-arrest-8-over-deepfake-scams-bypassing-bank-security-checks

[23] FBI IC3. Public Service Announcement I-120324-PSA. "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud." December 3, 2024. https://www.ic3.gov/PSA/2024/PSA241203

[24] FBI. "Senior U.S. Officials Impersonated in Malicious Messaging Campaign." May 15, 2025. https://www.fbi.gov/investigate/cyber/alerts/2025/senior-us-officials-impersonated-in-malicious-messaging-campaign

[25] CrowdStrike. 2025 Global Threat Report. February 2025.

Additional Federal Agency Source

[7a] Federal Trade Commission. Protecting Older Consumers 2024–2025: A Report of the Federal Trade Commission. December 1, 2025. https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf

ABOUT

About This Report

The Vanishing Red Flag Report is an independent research publication examining the evolving intersection of generative AI and consumer fraud.

It analyzes how advances in synthetic media, automation, and large-scale personalization are reshaping fraud dynamics across existing scam categories.

This report is produced by **ZeroScam™ Research**, an analytical initiative focused on emerging fraud patterns and risk signals in digital communications.

Methodology

This analysis synthesizes publicly available data from official U.S. federal agency publications (FTC Consumer Sentinel Network, FBI IC3 Annual Reports), peer-reviewed academic research, and established industry reports from recognized firms (Chainalysis, Feedzai, Sumsub, Mastercard, GASA, Gartner).

Industry data is cited as directional indicators of AI adoption in fraud — not as official loss attribution.

No proprietary datasets, internal telemetry, or unverified estimates were used in the preparation of this report.

Scope

This publication evaluates high-level structural trends and documented case studies. It does not describe operational techniques or vulnerabilities in actionable detail.

Contact

For press inquiries, interviews, or citation permissions:

press@zeroscam.io

zeroscam.io/research

Published February 2026. Version 2.0.