International Journal of Computer Applications (0975 - 8887)
Volume 187 - No.98, April 2026

The Marketing-Fraud Convergence: When Legitimate AI Tools Enable Financial Crime

Francis Martinson
Department of Computer Science
North Dakota State University, USA
ORCID: 0009-0007-2235-2516

ABSTRACT

The rapid commercialization of generative AI has created a troubling convergence: the same synthetic media tools marketed for legitimate business applications, including AI avatars for marketing videos, voice cloning for content localization, and video generation for advertising, provide identical capabilities exploited for financial fraud, identity theft, and social engineering attacks. This paper analyzes this marketing-fraud convergence through systematic examination of current synthetic media platforms and documented fraud cases. Building on the Authenticity Spectrum Framework (ASF) introduced in prior work [1], the analysis demonstrates that architectural similarities between marketing and fraud applications create fundamental governance challenges that platform-level controls alone cannot address. Analysis of representative platforms reveals that tools generating synthetic user-generated content for advertising operate on identical technical principles to systems enabling deepfake business email compromise, synthetic identity fraud, and investment scams. This paper presents a dual-use risk assessment framework enabling financial institutions, platform operators, and regulators to evaluate synthetic media services for fraud potential. The framework maps specific technical capabilities to established financial crime vectors, providing actionable guidance for compliance and risk management programs.

General Terms

AI Security, Financial Crime, Risk Assessment

Keywords

Synthetic Media, Financial Fraud, Deepfakes, AI Governance, Dual-Use Technology, Identity Fraud, Voice Cloning, Business Email Compromise

1. INTRODUCTION

In January 2024, fraudsters executed what may be the largest known deepfake-enabled theft: $25 million stolen from the Hong Kong office of British engineering firm Arup through a video conference call featuring AI-generated recreations of the company's chief financial officer and other executives. The employee who authorized the transfers believed he was participating in a legitimate multi-party video meeting. Every other participant was synthetic. This incident exemplifies a troubling convergence in generative AI: the same technologies marketed for legitimate business applications, including AI avatars for corporate communications, voice cloning for content production, and video generation for marketing, provide identical capabilities exploited for sophisticated financial crimes.

The synthetic media industry has grown rapidly, with platforms explicitly marketing AI-generated content for commercial applications. Services like Synthesia, HeyGen, and D-ID offer AI avatars for corporate training and marketing videos. Platforms such as MakeUGC, Creatify, and Arcads generate synthetic user-generated content for advertising campaigns. Voice cloning services including ElevenLabs and Resemble AI enable audio content production at scale. Video generation models from Runway, Pika, and emerging services create photorealistic synthetic footage. These applications are legitimate, valuable, and increasingly mainstream.

However, the technical capabilities enabling these business applications are architecturally identical to those enabling fraud. The AI avatar generating a product testimonial uses the same face synthesis techniques as deepfake impersonation attacks. The voice cloning service producing localized marketing content operates on the same neural architectures enabling vishing (voice phishing) attacks. The video generation model creating advertising footage can equally fabricate evidence of events that never occurred. This is not a matter of misuse; it is a fundamental characteristic of the underlying technology.

This paper analyzes the marketing-fraud convergence through systematic examination of current platforms and documented fraud cases. Building on the Authenticity Spectrum Framework (ASF) introduced in prior research [1], the analysis demonstrates that platform-level controls cannot fully address risks inherent in dual-use synthetic media capabilities. This paper presents a framework for assessing fraud potential in synthetic media services, providing guidance for financial institutions, platform operators, and regulators.

1.1 Research Objectives

This research pursues four objectives: (1) document the technical convergence between marketing-oriented and fraud-enabling synthetic media capabilities; (2) analyze how legitimate platform features map to established financial crime vectors; (3) develop a dual-use risk assessment framework for evaluating synthetic media

services; (4) provide actionable guidance for compliance and risk management programs.

2. BACKGROUND AND RELATED WORK

2.1 The Synthetic Media Ecosystem

The current synthetic media ecosystem encompasses several distinct but overlapping technology categories, each with legitimate commercial applications and corresponding fraud potential. AI Avatar platforms generate photorealistic digital humans from text scripts. Commercial applications include corporate training, marketing videos, and customer service automation. The same technology enables fake video testimonials and impersonation attacks.
Voice cloning services synthesize speech matching specific voice characteristics from minimal training samples. Commercial applications include audiobook production, content localization, and accessibility features. Identical capabilities enable voice phishing attacks and CEO fraud schemes. Video generation models create synthetic footage from text descriptions or reference images. Commercial applications include advertising production and content creation. The same models can fabricate evidence of events that never occurred.
Face generation systems produce photorealistic images of nonexistent individuals. Commercial applications include stock photography and privacy-preserving imagery. These systems provide the foundation for synthetic identity fraud, creating fake persons with AI-generated faces for fraudulent account applications.

2.2 Financial Crime Context

Synthetic media has emerged as a significant enabler of financial crime across multiple vectors. Business Email Compromise (BEC) attacks have evolved from text-based impersonation to video and voice deepfakes, dramatically increasing their effectiveness. The Arup case demonstrates the potential scale of deepfake-enabled BEC. Synthetic identity fraud, creating fictitious identities using AI-generated faces and fabricated credentials, has grown to an estimated $6 billion annually in the United States alone [2]. Voice cloning enables vishing attacks impersonating family members, executives, or authority figures.

2.3 Regulatory Context

Financial regulators have begun addressing synthetic media risks. The Federal Reserve has issued guidance on synthetic identity fraud detection. The FTC has warned about AI-enabled impersonation scams. The EU AI Act establishes disclosure requirements for deepfakes depicting real persons [3]. However, regulatory frameworks struggle to address the fundamental dual-use nature of synthetic media, as the same technologies serve both legitimate commerce and criminal exploitation.

3. METHODOLOGY

3.1 Platform Analysis

This study conducted systematic analysis of synthetic media platforms across five categories during the period January-March 2026. The categories examined included: AI avatar generators (Synthesia, HeyGen, D-ID, MakeUGC, Creatify, Arcads), voice cloning services (ElevenLabs, Resemble AI, Speechify, Play.ht), video generation models (Runway Gen-3, Pika, Kling, Luma), face generators (Midjourney, DALL-E, Stable Diffusion, ThisPersonDoesNotExist), and LLM-based text generation (GPT-4, Claude, Gemini). For each platform, the analysis documented four dimensions: (a) technical capabilities including input requirements, output quality, and customization options; (b) stated commercial applications as presented in marketing materials; (c) access controls and verification requirements; and (d) potential fraud applications based on capability mapping to known crime vectors. Platform selection prioritized services with significant market adoption and documented commercial deployment.

3.2 Fraud Case Analysis

This research analyzed 47 documented fraud cases involving synthetic media published between 2022 and 2026. Sources included regulatory enforcement actions from the FTC, SEC, and international equivalents; law enforcement reports from the FBI IC3 and Europol; academic case studies; and verified news coverage of significant incidents. Cases were categorized by synthetic media modality (voice, video, image, or multimodal), fraud type (BEC, identity fraud, investment scam, or romance fraud), confirmed or estimated financial impact, and detection method. Inclusion criteria required documented financial loss exceeding $10,000 and confirmed synthetic media involvement.

3.3 Framework Development

The dual-use risk assessment framework was developed through iterative mapping of platform capabilities to fraud vectors identified in case analysis. Development involved three phases: (1) capability extraction from platform documentation and testing, (2) crime vector mapping based on case analysis, and (3) risk factor validation against the Authenticity Spectrum Framework [1] classification scheme. Risk factors were weighted based on exploitation frequency in documented cases and potential financial impact. The framework was validated through application to 15 platforms not included in initial analysis.

4. RESULTS: MARKETING-FRAUD CONVERGENCE

Analysis reveals systematic convergence between marketing applications and fraud capabilities across all synthetic media categories. Table 1 summarizes the convergence patterns.

Table 1. Marketing-Fraud Convergence Matrix

Technology	Marketing Use	Fraud Use	Risk
AI Avatars	Product testimonials, Corporate training	Executive impersonation, Fake endorsements	HIGH
Voice Cloning	Content localization, Audiobooks	Vishing, CEO fraud	HIGH
Face Generation	Stock photography, Privacy images	Synthetic identity fraud	HIGH
Video Generation	Marketing content, Advertising	Evidence fabrication, Scam videos	MED

4.1 AI Avatars: From Testimonials to Impersonation

AI avatar platforms marketed for creating marketing testimonials and corporate communications provide capabilities directly applicable to impersonation attacks. Analysis of MakeUGC, Creatify, and Arcads reveals features explicitly designed for generating synthetic user-generated content. These platforms generate AI avatars delivering scripted product endorsements that are visually indistinguishable from recordings of human customers. Testing across six major platforms revealed average generation times under 60 seconds and output quality sufficient to pass casual inspection. Four of six platforms offered no identity verification for avatar subjects, enabling creation of synthetic content featuring arbitrary individuals.

The same authenticity that makes synthetic testimonials effective for marketing makes them effective for fraud. Fake customer reviews, fraudulent investment endorsements, and impersonation of authority figures become trivially achievable. Platform safeguards, including terms of service prohibitions and content moderation, cannot prevent misuse when the core value proposition is indistinguishability from authentic human content.

4.2 Voice Cloning: From Localization to Vishing

Voice cloning services marketed for content localization and accessibility enable sophisticated voice phishing attacks. Analysis of four major platforms revealed that services requiring only 10-30 seconds of reference audio provide sufficient quality for telephone-based impersonation. Real-time voice conversion capabilities, available in two of four platforms tested, enable live conversation with cloned voices. The $25 million Arup theft reportedly involved cloned voices of multiple executives, demonstrating operational deployment of these capabilities. Testing confirmed that current-generation voice clones are perceptually indistinguishable from authentic speech in telephone-quality audio conditions.

Financial institutions report increasing volume of AI-generated voice attacks. Some major retailers report receiving over 1,000 AI-generated scam calls daily. The perceptual cues that once distinguished synthetic from authentic voices have largely disappeared in current-generation systems.

4.3 Synthetic Identity Fraud

Face generation capabilities marketed for stock photography and privacy-preserving imagery enable synthetic identity fraud at scale. Current face generators produce photorealistic images at resolutions exceeding identity document requirements. Analysis found that AI-generated faces successfully passed automated liveness detection in 3 of 5 commercial verification systems tested. Unlike stolen identities, synthetic identities have no victim to report the fraud, enabling extended exploitation before detection. The Federal Reserve estimates synthetic identity fraud losses at $6 billion annually in the United States, with AI-generated faces increasingly replacing manually composited images.

5. FINANCIAL CRIME VECTOR ANALYSIS

Mapping synthetic media capabilities to established financial crime categories reveals systematic exploitation patterns. Table 2 summarizes major crime vectors with estimated financial impacts.

Table 2. Financial Crime Vectors Enabled by Synthetic Media

Crime Vector	Synthetic Media Type	Annual Impact
Business Email Compromise	Voice cloning, Video deepfakes	$2.9B (FBI IC3)
Synthetic Identity Fraud	AI-generated faces	$6B (Fed Reserve)
Investment Scams	Celebrity deepfakes	$4.6B (FTC)
Romance Fraud	AI personas, Voice cloning	$1.3B (FTC)

5.1 Business Email Compromise Evolution

Traditional BEC attacks relied on text-based impersonation, with spoofed emails directing wire transfers. Synthetic media has enabled BEC evolution to video and voice channels. The Arup incident demonstrates fully synthetic video conferencing, but voice-only attacks using cloned executive voices have become increasingly common. Detection difficulty increases dramatically when attackers can provide real-time audio or video impersonation.

5.2 Investment and Romance Fraud

Cryptocurrency and investment fraud increasingly employs synthetic celebrity endorsements. AI-generated videos of prominent figures promoting fraudulent investment schemes circulate widely on social media, with global losses from AI deepfake-enabled fraud estimated at $12 billion annually. Romance scams have incorporated AI-generated personas and voice cloning for telephone calls, extending the deception that previously relied solely on text communication.

6. DUAL-USE RISK ASSESSMENT FRAMEWORK

Based on convergence analysis, this paper presents a framework for assessing fraud potential in synthetic media services. Table 3 summarizes key risk factors.

Table 3. Dual-Use Risk Assessment Framework

Risk Factor	Low Risk	High Risk
Identity Binding	Generic avatars	Specific individual cloning
Disclosure Context	Platform-labeled synthetic	Presented as authentic
Financial Stakes	Low-value transactions	High-value authorizations
Verification Bypass	No biometric relevance	Defeats identity checks

6.1 Risk Factor Analysis

Identity Binding assesses whether synthetic content is tied to real individual identity. Generic AI avatars presenting scripted content pose lower risk than systems cloning specific individuals' likeness or voice. Disclosure Context evaluates whether platform or deployment context implies synthetic origin. Content presented as authentic human testimony poses higher risk than platform-contextualized synthetic media.

Financial Stakes considers the transaction values associated with potential fraud applications. Voice cloning for high-value wire transfer authorization poses higher risk than synthetic content for low-value consumer transactions. Verification Bypass examines whether capabilities can circumvent identity verification systems. AI-generated faces suitable for document fraud or biometric spoofing represent elevated risk.

6.2 Integration with ASF Classification

The dual-use risk framework complements the Authenticity Spectrum Framework [1] by adding financial crime-specific risk factors. ASF Level 3-5 content, including undisclosed, deceptive, or malicious synthetic media, maps to elevated fraud risk. However, even Level 2 content (contextually disclosed but realistic synthetic media) may enable fraud when extracted from original deployment context. Financial institutions should apply both frameworks in synthetic media risk assessment.

7. DISCUSSION

7.1 Implications for Platform Governance

The marketing-fraud convergence presents fundamental challenges for platform governance. Technical capabilities that create commercial value, including authenticity, realism, and ease of generation, simultaneously enable fraud. Platform-level controls including terms of service, content moderation, and usage monitoring provide incomplete mitigation. Determined adversaries can operate within policy boundaries while developing capabilities for later misuse.

7.2 Implications for Financial Institutions

Financial institutions must assume that synthetic media capabilities are available to adversaries and adapt verification and authentication processes accordingly. Voice-based verification is increasingly compromised by cloning capabilities. Video-based verification faces similar challenges. Multi-factor approaches incorporating behavioral analysis, device fingerprinting, and transaction pattern monitoring become essential complements to biometric verification.

7.3 Regulatory Implications

The dual-use nature of synthetic media complicates regulatory approaches. Prohibiting capabilities that serve legitimate commerce is impractical; enabling fraud prevention while preserving beneficial applications requires nuanced frameworks. The ASF [1] provides classification criteria for proportionate governance responses. Industry-specific guidance for financial services should map synthetic media risks to existing compliance frameworks.

8. CONCLUSION

This paper analyzed the convergence between marketing-oriented synthetic media applications and financial fraud capabilities. Through systematic examination of current platforms and documented fraud cases, the analysis demonstrated that legitimate commercial tools provide identical technical capabilities exploited for sophisticated financial crimes.

Building on the Authenticity Spectrum Framework [1], this paper presented a dual-use risk assessment framework enabling financial institutions, platform operators, and regulators to evaluate synthetic media services for fraud potential. The framework maps specific technical capabilities to established financial crime vectors including synthetic identity fraud, deepfake business email compromise, and AI-enabled investment scams.

As synthetic media capabilities continue advancing, the marketing-fraud convergence will intensify. Effective governance requires recognition that platform-level controls alone cannot address risks inherent in dual-use technologies. Financial institutions must adapt verification processes, regulators must develop nuanced frameworks, and the synthetic media industry must engage proactively with fraud prevention rather than treating it as an externality.

9. REFERENCES

[1] F. Martinson, "The Authenticity Spectrum Framework: Classifying Deepfake and Generative AI Risks in Synthetic Media," *International Journal of Computer Applications*, vol. 187, no. 88, pp. 34–38, 2026. DOI: 10.5120/ijca2026926538

[2] Federal Reserve, "Synthetic Identity Fraud in the U.S. Payment System," Federal Reserve Bank Reports, 2024.

[3] European Union, "Regulation (EU) 2024/1689 (AI Act)," *Official Journal of the EU*, 2024.

[4] F. Martinson and D. Rangel, "A Comprehensive Analysis of Game Hacking through Injectors," *International Journal of Computer Applications*, vol. 185, no. 33, pp. 56–63, 2023.

[5] A. M. Abukari, M. Amini, and F. Martinson, "A Revealed Architecture of Camera-based Attacks for Smartphones," *International Journal of Computer Applications*, vol. 185, no. 27, pp. 45–49, 2023.

[6] R. Chesney and D. K. Citron, "Deep fakes: A looming challenge," *California Law Review*, vol. 107, pp. 1753–1820, 2019.

[7] NIST, "AI Risk Management Framework," NIST AI 100-1, 2023.

[8] FTC, "Consumer Alert: AI Voice Cloning Scams," 2024.

[9] Y. Mirsky and W. Lee, "The creation and detection of deepfakes," *ACM Computing Surveys*, vol. 54, no. 1, pp. 1–41, 2021.

[10] FBI, "Internet Crime Report 2023," IC3, 2024.

[11] Deloitte, "Generative AI and Fraud Risk," Deloitte Insights, 2024.

[12] C. Vaccari and A. Chadwick, "Deepfakes and disinformation," *Social Media + Society*, vol. 6, no. 1, 2020.

[13] Partnership on AI, "Framework for Responsible Practices in Synthetic Media," 2023.

[14] J. Kietzmann *et al.*, "Deepfakes: Trick or treat?" *Business Horizons*, vol. 63, no. 2, pp. 135–146, 2020.

[15] M. Westerlund, "The emergence of deepfake technology," *Technology Innovation Management Review*, vol. 9, no. 11, 2019.