ONSEC

THE $25 MILLION VIDEO CALL

Why Deepfake Fraud Will Crush Unprepared iGaming

The Attack That Changed Everything

A finance employee received a video call from their CFO. The face was right. The voice was right. The request seemed urgent but reasonable: transfer $25 million to five bank accounts for a confidential acquisition.

It was all fake.

The "CFO" was a deepfake - an AI-generated video clone so convincing that even trained professionals couldn't tell the difference. The money vanished.

This wasn't a hypothetical. It happened. And iGaming platforms - with VIP accounts, crypto wallets, and high-roller payouts - are the next prime targets.

High-value targets:

- VIP player accounts with six-figure balances
- Crypto withdrawals that can't be reversed
- Affiliate payouts running into millions monthly
- White-label operators with limited security

resources

Perfect attack conditions:

- Remote verification for KYC and account recovery
- Video calls for VIP account managers and

high-roller support

- Pressure to process withdrawals quickly
- Multiple time zones = harder to verify in real-time

The Numbers That Should Terrify You

- 700% year-over-year increase in deepfake fraud (U.S. Federal Trade Commission)
- $12.5 billion in U.S. financial fraud losses in 2025, with AI-assisted attacks driving the surge
- 30% of enterprises will no longer trust standalone identity verification by 2026 (Gartner prediction)
- 1,100 deepfake fraud attempts against a single Indonesian financial organization
- $25 million stolen in one deepfake video call attack

Deepfake-as-a-Service: The Democratization of Fraud

In 2025, Deepfake-as-a-Service (DaaS) platforms exploded.

What this means:

- No technical skills required
- Voice cloning from 3 seconds of audio
- Real-time face-swapping during live calls
- Subscription models starting at $20/month

Attackers no longer need sophistication. They need a credit card.

ONSEC has observed DaaS being used to:

- Clone CEO voices for payment authorization
- Generate synthetic identities for KYC bypass
- Create fake "verification selfies" for account

takeover

- Impersonate support agents on live chat

1. VIP Account Takeover

Attacker generates deepfake of a high-roller using social media photos and voice samples from public appearances. Calls VIP support requesting emergency withdrawal.

2. KYC Bypass

Synthetic identity with AI-generated documents and live deepfake for video verification. Opens multiple accounts for bonus abuse or money laundering.

3. Executive Impersonation

Deepfake CFO or CEO authorizes fraudulent payouts, vendor payments, or affiliate settlements during video calls.

4. Affiliate Fraud

Fake affiliates with synthetic identities claim referral bonuses at scale.

5. Internal Compromise

Attacker joins internal Zoom/Teams meeting as a trusted colleague, uses shared screen to direct

malicious actions.

Why Traditional Security Fails

MFA won't save you - deepfakes target human verification, not system authentication

KYC video calls are compromised - real-time deepfakes can pass live checks

Voice verification is broken - 3 seconds of audio is enough to clone a voice

Training isn't keeping up - employees are trained to spot phishing emails, not convincing video calls

Implement dual-control for high-value actions:

- No single person can authorize payouts above

threshold

- Mandatory callback verification via separate channel

- Time delays on large withdrawals (even for VIPs)

Upgrade verification protocols:

- Out-of-band confirmation for all video call requests
- Pre-shared code words for executive

communications

- Liveness detection that tests for AI artifacts

Build deepfake awareness:

- Train staff specifically on AI-generated content
- Run deepfake phishing simulations
- Create escalation paths for suspicious calls

Technical countermeasures:

- Audio/video analysis tools for deepfake detection
- Behavioral biometrics for account access
- IP and device fingerprinting for session validation

ONSEC's Approach to Deepfake Defense

ONSEC's red team engagements now include:

- Deepfake simulation attacks targeting VIP support

and finance teams

- Social engineering tests using AI-generated voice

and video

- KYC bypass attempts with synthetic identities
- Executive impersonation scenarios via video

conference

We show you exactly how attackers would exploit your people - before they do.

The Bottom Line

Deepfake fraud isn't coming. It's here.

The $25 million loss from one video call is just the beginning. iGaming platforms combine everything attackers want: high-value transactions, time pressure, remote operations, and human verification points.

By end of 2026, deepfakes will be the default social engineering tool.

The question isn't whether your platform will face a deepfake attack. It's whether your team will recognize it when it happens.

ONSEC tests your defenses against the attacks that are actually coming - not the ones from five years ago.

Sources:

- U.S. Federal Trade Commission - Deepfake fraud statistics
- Gartner - Identity verification predictions 2026
- Cyble - Deepfake-as-a-Service research 2025
- SecurityWeek - Five Cybersecurity Predictions for 2026
- ONSEC.io - Razor-Sharp Security for iGaming

ONSEC

About ONSEC

ONSEC is a boutique penetration testing and security assessment team specializing in iGaming platforms. We help operators identify vulnerabilities in APIs, payment systems, and player-facing applications before attackers do—whether the risk is fraud, data exposure, or regulatory non-compliance. Our team has worked with casinos, sportsbooks, and gaming providers across multiple jurisdictions. If you'd like to discuss how we can help strengthen your platform, reach out to schedule a quick call.

Our Services:

✓ Penetration Testing — Full-scope security assessments of your platform, APIs, and mobile apps

✓ iGaming Security Audits — Compliance-focused reviews for UKGC, MGA, and other regulators

✓ Fraud & AML Assessment — Evaluate your defenses against bonus abuse, multi-accounting, and money laundering

✓ Incident Response — 24/7 support when security incidents occur

✓ Security Architecture Review — Design secure systems from the ground up

✓ Dark Web Monitoring — Track your brand and player credentials on underground markets

https://onsec.io • request@onsec.io

ONSEC.io — Razor-Sharp Security for iGaming

Trusted by leading organizations worldwide.