The Risk of Fraudulent Deepfake Attacks in the Sports Ticketing Supply Chain

TIAKI

80%+ of fraud experts agree that deepfake attacks are becoming a critical risk to the business

The era of deepfake cyber attacks has arrived. The impact on global sports franchises that have just signed billion dollar media rights deals can be profound. **As deepfake incidents continue to rise in 2024, with a predicted increase of 60% or more this year**, the number of global cases is expected to reach 150,000 or more, establishing **AI-powered deepfake attacks as the fastest-growing type of adversarial AI currently**. Leading research forecasts that these **deepfake attacks could lead to over $40 billion in damages by 2027[1].**

One-Third of Global Businesses Were Hit by Voice and Video Deepfake Fraud in 2023:

A recent survey conducted by Regula [2] in countries such as the United States, the United Kingdom, France, and Germany, revealed that a significant number of businesses worldwide have already been impacted by voice and video deepfake fraud.

The survey found that 37% of organisations have encountered deepfake voice fraud, while 29% have fallen victim to deepfake videos. The proliferation of AI capability within the cybercriminal ecosystem has made it easier to create convincing deepfakes, posing a serious fraud challenge for the ticketing supply chain in the sports industry.

The survey also highlighted that 80% of companies view fake biometric artifacts such as deepfake voice or video as genuine threats. Particularly in the United States, where 91% of organizations perceive this type of fraud as a growing concern.

In the survey, 46% of respondents encountered instances of synthetic identity fraud, where a blend of authentic and fabricated identity elements, like a counterfeit social security number paired with a genuine name, address, and birth date, was utilised.

The increasing risk is clearly a growing concern with **80-90% of fraud experts in the survey agreeing that synthetic identity fraud, voice deepfakes and video deepfakes are now a genuine threat to the business.**

The combination of the influx of private equity and substantial billion-dollar sports media rights deals raises concerns about leading sports leagues such as those in the NFL, MLB, NBA, NHL, Premier League, IPL, and Rugby Championship. These organisations might now be at greater risk and perceived as easy targets by AI-powered cyber criminals. Given this scenario, implementing Secure Access Service Edge (SASE) can play a crucial role in neutralising the threat posed by AI-powered deep fake attacks in the sports industry ticketing ecosystem.

---

[1] https://venturebeat.com/security/deepfakes-will-cost-40-billion-by-2027-as-adversarial-ai-gains-momentum/
[2] One-Third of Businesses Hit by Voice and Video Deepfake Fraud (regulaforensics.com)

Understanding the deepfake threat

AI-powered deepfake attacks have emerged as a potent weapon in the hands of cybercriminals, enabling them to create highly realistic and deceptive audio, video, or text content that can be used to spread misinformation, manipulate public opinion, or deceive individuals. For high-profile sports franchises that have just signed billion-dollar media rights deals, the potential impact of deepfake attacks on their reputation, financial stability, and fan base cannot be underestimated.

In the contemporary commercial landscape, AI advancements like Generative AI and deepfakes have transformed from simple misinformation tools into sophisticated instruments of deception. The increasing sophistication of AI has made it progressively difficult to differentiate between authentic and manipulated information.

In a recent C-suite survey, **62% of CEOs and senior business executives, anticipate that deepfakes will introduce operational costs and complexities for their organisations within the next three years, with 5% viewing it as an existential threat. Gartner forecasts that by 2026, the utilisation of AI-generated deepfakes in face biometrics attacks will lead to 30% of enterprises no longer considering these identity verification and authentication solutions as reliable in isolation[3].**

The increasing deepfake risk to the sport ticketing ecosystem

The risk of deepfake attacks into the ticketing supply chain for high-profile sports franchises can have significant consequences. Here are some potential risks associated with deepfake attacks in the sports ticketing supply chain:

1. Fraudulent ticket sales:
Deepfake attacks can be used to create fake tickets that are indistinguishable from genuine ones. This can lead to fraudulent ticket sales, resulting in financial losses for both the sports franchise and fans who purchase counterfeit tickets.

2. Identity theft:
Deepfake technology can be used to create fake identification documents, which can be used to purchase tickets under false identities. This can lead to identity theft and unauthorized access to sensitive information.

3. Ticket scalping:
Deepfake attacks can be used by ticket scalpers to manipulate ticket prices and create artificial scarcity. This can result in inflated ticket prices and limited access to genuine tickets for fans.

4. Disruption of ticketing systems:
Deepfake attacks can disrupt the ticketing systems of sports franchises, leading to technical glitches, system failures, and delays in ticket sales. This can impact the fan experience and result in dissatisfaction among ticket buyers.

5. Reputational damage:
If deepfake attacks target the ticketing supply chain of a high-profile sports franchise, it can damage the

[3] Gartner Predicts 30% of Enterprises Will Consider Identity Verification and Authentication Solutions Unreliable in Isolation Due to AI-Generated Deepfakes by 2026

reputation of the team and erode trust among fans and stakeholders. This can have long-term consequences on the franchise's brand image and financial performance.

Overall, deepfake attacks in the ticketing supply chain pose a significant risk to high-profile sports franchises, highlighting the importance of implementing robust cybersecurity measures to protect against such threats.

A comprehensive SASE strategy can reduce the deepfake risks

A Secure Access Service Edge (SASE) strategy specifically addresses the risk of AI-augmented deepfake fraud attacks in the sports ticketing supply chain by providing a comprehensive and integrated approach to cybersecurity that combines networking and security capabilities into a single cloud-based service. Here's how a SASE strategy can address this specific risk:

1. Identity Verification:
SASE solutions incorporate strong identity verification mechanisms, such as multi-factor authentication and biometric authentication, to ensure that only authorised individuals can access ticketing systems. This helps prevent unauthorised access by fraudsters using deepfake technology to impersonate legitimate users.

2. Zero Trust Architecture:
SASE follows a zero trust security model, which means that all users and devices are treated as untrusted until proven otherwise. This approach minimises the risk of deepfake fraud attacks by requiring continuous verification of user identities and device integrity before granting access to ticketing systems.

3. Data Encryption:
SASE solutions include robust data encryption capabilities to protect sensitive ticketing data from interception and manipulation by malicious actors leveraging deepfake technology. Encryption ensures that even if fraudsters gain access to the data, they cannot decipher or alter it.

4. Threat Detection and Response:
SASE platforms integrate advanced threat detection and response mechanisms, such as AI-driven analytics and real-time monitoring, to identify and mitigate deepfake fraud attacks in real-time. By detecting anomalies and suspicious activities, SASE helps organisations respond swiftly to potential threats before they escalate.

5. Secure Connectivity:
SASE provides secure connectivity for remote users and branch offices, ensuring that all network traffic is encrypted and inspected for potential threats. This protects against unauthorised access and data breaches that could result from deepfake fraud attacks targeting the sports ticketing supply chain.

6. Comprehensive Security Policies:
SASE allows organisations to enforce consistent security policies across all network, IoT and cloud environments, including ticketing systems. This ensures that security measures are applied uniformly to prevent vulnerabilities that could be exploited by deepfake fraudsters.

A SASE strategy addresses the risk of AI-augmented deepfake fraud attacks in the sports ticketing supply chain by integrating multiple security measures, such as identity verification, zero trust architecture, data

encryption, threat detection, secure connectivity, and comprehensive security policies. By adopting a SASE approach, sports franchises can enhance their cybersecurity posture and protect their ticketing systems from the evolving threat landscape posed by deepfake technology.

Conclusion:

The cybersecurity risks posed by AI-augmented deepfake attacks on sports franchise ticketing supply chains are real and evolving. By embracing Secure Access Service Edge (SASE) as a comprehensive cybersecurity solution, sports organisations can enhance their resilience against these sophisticated threats, safeguard their reputation, and protect their valuable assets. With SASE's integrated approach to network security and access control, sports franchises can stay ahead of the curve and ensure a secure digital environment for their stakeholders, fans, partners and investors.

About the Author:

David Andrew
Founder & Managing Partner
www.tiaki.ai
david.andrew@tiaki.ai

David is the Founder & Managing Partner at TIAKI, a niche consulting practice helping executive leadership in sport make confident, informed decisions on their risks, investments and business outcomes powered by secure 'data-at-scale'.
He collaborates with bold and determined leaders in the sports ecosystem to define their data, AI and cybersecurity strategies to deliver sustainable value.

David's vision for TIAKI is to empower sports franchise CEOs, leadership teams, sports media broadcasters and investors in the global sports industry with strategic advisory frameworks to deliver secure, pioneering digital fan experiences and new ecosystem business models to achieve breakthrough returns.

David has over 20 years of strategy and technology enabled business transformation experience, providing consulting expertise in cloud native technologies, data strategy, digital business enablement and cybersecurity strategy. He is passionate about helping talented leadership teams succeed in securely growing their differentiated business models in the data-driven, digital sports economy.

Based in Stockholm, David previously worked for IBM Consulting, EY, Accenture Strategy and Orange Business. He studied Chemistry at Durham University and holds an MBA from Trinity College, Dublin Business School.