BLOG REPORT

Agentic Apocalypse: How Google's AI Checkout Unleashes a ‘Deepfake Tsunami’ on Sports Ticketing

TIAKI

The Existential Threat: How AI-Augmented Google Search and Deepfakes Jeopardize the Global Sports Ticketing Supply Chain

The digital landscape of sports ticketing is on the brink of a seismic shift, one that poses an existential threat to the industry's integrity and financial stability. Google's recent announcement of "agentic checkout" within its AI-augmented Search, allowing users to complete purchases directly within search results, is a game-changer. While promising unparalleled convenience, this development simultaneously opens a Pandora's Box of deepfake fraudulent risks, threatening to overwhelm the global sports ticketing supply chain ecosystem.

The Dawn of Agentic Checkout: Convenience vs. Catastrophe

At the Google I/O developer conference (20-21st May 2025), "AI Mode" was unveiled with features such as "Deep Search" and AI-powered shopping tools, including automated purchasing, signaling a new era of online transactions.

The concept of "agentic checkout" empowers AI to complete purchases on a user's behalf, leveraging tools like Google Pay. This seamless, direct-from-search purchase capability, while designed for user convenience, inadvertently creates fertile ground for sophisticated cybercriminal exploitation.

Imagine a world where a sports fan searches for tickets, and an AI agent, powered by Google's advanced models, handles the entire transaction—from finding the best seats to finalizing the purchase. Now, imagine this same capability weaponized by malicious actors. The removal of traditional checkout page friction, while appealing to legitimate users, also removes layers of security checks and human oversight that often act as deterrents to fraud.

The Global Sports Ticketing Juggernaut: A High-Stakes Target

To understand the magnitude of this threat, one must grasp the sheer scale of the global sports ticketing market. This industry is a multi-billion dollar behemoth, constantly growing and attracting massive fan engagement.

Global Market Size:

The global sports events ticket market was estimated at a staggering **$61 billion** in 2023 and is projected to reach an impressive $115.0 billion by 2032, growing at a Compound Annual Growth Rate (CAGR) of 7.28% from 2024 to 2032. North America leads this market, accounting for over 35% of the market share in 2023, with the U.S. online event ticketing market alone projected to reach $39.8 billion in 2027.[1]

North American Leagues:

- ★ **NFL:** Ticketing and luxury suites generated an estimated **$3.5 billion** (17% of total revenue) in 2023.
- ★ **NBA:** Ticket revenue hit **$2.9 billion** in the 2022-2023 season. Estimates for 2023-2024 project at least **$3.4 billion** (26% of total revenue).
- ★ **MLB:** Analysts estimate ticket sales at approximately **$4 billion** (31% of total revenue) in a market valued at $13 billion in 2024.
- ★ **NHL:** Ticketing sales were an estimated **$2.7 billion**, accounting for a significant 44% of total

[1] Sports Events Ticket Market Size, Share, Trends, Report Analysis

2023-2024 revenue.

★ **MLS:** Ticketing revenues are estimated at **$1 billion** (40% of total revenue) in a market valued at $2.6 billion in 2024.

European Football Powerhouses:

- **Premier League:** Clubs collectively generated nearly **$1 billion** from home match ticket sales in 2023, growing 10% annually.
- **European Champions League:** This competition significantly drives ticketing revenues estimated at **$8.4 billion** or 30% of the global secondary ticketing market at **$28 billion** which is projected to reach $73 billion by 2033.
- **FIFA World Cup:** FIFA aims for at least **$1.8 billion** in ticketing revenue for the 2026 World Cup.

This huge market, with its high demand and premium pricing for sought-after events, becomes an irresistible target for cybercriminals, especially when new vulnerabilities are introduced.

The Revenue at Risk: A Sobering $13 Billion Estimate

Given the new "agentic checkout" model and the sophisticated capabilities of AI-powered deepfakes, it's reasonable to estimate that a significant portion of the sports ticketing supply chain revenue is now at heightened risk. While a precise percentage is difficult to quantify without historical data specific to this new threat vector, we can infer the potential impact.

Considering the rapid advancements in AI fraud and the frictionless nature of agentic checkout, it's plausible that **$13 billion or 20% of the current global sports ticketing revenue, could be directly or indirectly exposed to elevated deepfake fraudulent risks.** This estimate accounts for:

- **Increased volume of fraudulent transactions:** AI agents can automate and scale fraudulent purchases at an unprecedented rate, far exceeding human capabilities.
- **Sophisticated social engineering:** Deepfakes (audio, video, text) can create highly convincing impersonations of legitimate sellers, venues, or even official ticket agencies, tricking buyers into purchasing fake tickets or divulging sensitive information.
- **Identity theft and account takeover:** AI-powered deepfakes can facilitate more effective phishing and vishing attacks, leading to compromised fan accounts or payment details.
- **Market distortion:** Bots, now "supercharged" by advanced AI agents, can hoard legitimate tickets, driving up prices on secondary markets and making it harder for genuine fans to access events, while deepfake-backed fraudulent sales flood these markets with invalid tickets.[2]

[2] Protecting consumers from AI bot ticket and public services hoarding - World ID

In our Blog Report, [The Risk of Fraudulent Deepfake Attacks in the Sports Ticketing Supply Chain - TIAKI](), we discuss how deepfake technology is creating a significant vulnerability in the sports ticketing supply chain, enabling fraudsters to create convincing fake videos and audio to manipulate ticket sales and deceive consumers.

These fraudulent attacks can lead to substantial financial losses, erode trust in ticketing platforms, and disrupt the integrity of sporting events.

Sports properties and ticketing platforms must implement advanced authentication and verification measures to combat these deepfake threats and protect both consumers and the industry.

Deepfake Attacks: A Cybercriminal's New Playbook

Deepfakes are synthetic media in which a person in an existing image or video is replaced with someone else's likeness. While often associated with video, deepfakes can also be audio or text-based, creating highly convincing, yet entirely fabricated, content.

How Deep Fakes Amplify Ticketing Fraud with Agentic AI Checkout

1. **Impersonation for Account Takeover and Phishing:**
    - **Fake Customer Support:** A cybercriminal could use a deepfake voice or video to impersonate a legitimate ticketing agent or customer support representative. They could contact a fan, perhaps claiming there's an issue with their recent agentic purchase, and "guide" them through a fraudulent verification process to steal credentials or payment information.
    - **"Official" Communications:** Deepfakes could be used to create highly convincing fake emails or messages from sports properties or ticketing platforms, prompting fans to click on malicious links or make payments to fraudulent accounts, especially when the AI agent handles the checkout process.
    - **Fake Seller Profiles:** On secondary marketplaces, deepfakes could be used to create highly credible, yet entirely fake, seller profiles with convincing backstories and even "proof" of ticket ownership, deceiving buyers who rely on visual or audio cues for legitimacy.

2. **Automated Fraudulent Purchases:**
    - **Bypassing Human Verification:** As AI-driven automated purchasing becomes more prevalent, cybercriminals can train their own AI agents, enhanced with deepfake capabilities (e.g., generating fake IDs for verification purposes), to rapidly purchase large quantities of tickets directly through "agentic checkout" functionalities. These tickets can then be resold fraudulently.
    - **Circumventing Bot Protection:** Current bot protection mechanisms, like CAPTCHAs, are increasingly ineffective against advanced AI. Deepfake technology can create synthetic identities that can bypass more sophisticated verification methods, making it even harder to distinguish between a legitimate human buyer and a fraudulent AI agent.[3]
3. **Disinformation and Market Manipulation:**
    - **Spoofed Announcements:** Deepfakes could be used to create fake announcements from sports teams or venues about ticket releases, cancellations, or changes, manipulating fan behavior to falsely cause a spike in market demand or driving traffic to fraudulent sites.
    - **Damaging Brand Reputation:** Malicious actors could spread deepfakes depicting forged incidents or statements from sports properties, eroding fan trust and creating chaos in the ticketing ecosystem.[4]

The "agentic checkout" feature, by design, seeks to reduce friction. However, in the context of deepfake fraud, this reduced friction means fewer opportunities for human or system intervention to detect and prevent fraudulent activities, effectively handing cybercriminals a more efficient pipeline to exploit the sports ticketing supply chain.

10 Strategic and Operational Actions for Sports Properties

To mitigate the rising risks posed by AI-augmented Google Search and deepfake fraud, sports properties must adopt a proactive, multi-layered approach to cybersecurity, data management, and fan education.

1. **Develop a Comprehensive Data, AI & Cybersecurity Strategy:** This is foundational. Sports organizations must integrate cybersecurity considerations into their overall business strategy, focusing on protecting fan data, transaction integrity, and brand reputation. This includes understanding their data landscape, implementing AI-driven security measures, and creating a robust incident response plan.[5]
2. **Adopt Secure Access Service Edge (SASE) Best Practices:** SASE unifies networking and security functions into a single, cloud-native service. For sports properties with distributed operations (venues, remote staff, online platforms), SASE provides consistent security, zero-trust network access (ZTNA), data loss prevention (DLP), and firewall-as-a-service (FWaaS), protecting sensitive data and access points across the entire ecosystem.[6]
3. **Implement Advanced AI-Powered Fraud Detection and Prevention:** Leverage AI and machine learning to analyze transaction patterns, identify anomalies, and detect fraudulent activities in real-time. This includes behavioral analytics, device fingerprinting, and dynamic risk scoring for every transaction.
4. **Strengthen Identity Verification for High-Value Transactions:** For premium tickets or large purchases, implement multi-factor authentication (MFA) and consider advanced identity verification solutions that are resistant to deepfake impersonations, potentially integrating with "Proof of Human"

---

[3] Protecting consumers from AI bot ticket and public services hoarding - World ID
[4] Deepfake threats to companies - KPMG International
[5] Cyber protection in professional sports: How data and technology are changing the game - Acronis, 5 Ways AI Elevates Sports Analytics (Top Stats)
[6] Best Practices for Successful SASE Deployment - Check Point Software

technologies like World ID to prevent bot hoarding.[7]

5. **Educate Fans on Deepfake Risks and Safe Ticketing Practices:** Launch extensive awareness campaigns to inform fans about the dangers of deepfakes, phishing scams, and unofficial ticketing channels. Emphasize purchasing tickets only from verified official sources and advise caution against deals that seem "too good to be true."
6. **Enhance API Security and Authentication for Ticketing Platforms:** Given that Google's agentic checkout interacts with ticketing platforms via APIs, robust API security is paramount. Implement strong authentication, authorization, and continuous monitoring of API traffic to prevent unauthorized access and exploitation.
7. **Foster Collaboration and Information Sharing within the Industry:** Establish a cross-industry task force or intelligence-sharing platform where sports properties, ticketing companies, and cybersecurity experts can share threat intelligence, best practices, and collaborate on developing industry-wide defenses against AI-powered fraud.
8. **Regularly Conduct Penetration Testing and Vulnerability Assessments:** Proactively identify and address security weaknesses in ticketing systems, websites, and associated infrastructure. These tests should specifically simulate advanced AI-driven and deepfake-based attack scenarios.
9. **Develop a Rapid Incident Response and Communication Plan for Fraud Events:** Have a clear, actionable plan for responding to detected fraud, including immediate communication with affected fans, law enforcement, and relevant payment processors. Transparency and swift action are crucial for maintaining fan trust.
10. **Explore Blockchain and NFT Ticketing Solutions:** Investigate the potential of blockchain and non-fungible token (NFT) ticketing, which can provide immutable records of ownership, enhance traceability, and potentially reduce the prevalence of fake tickets and illicit resales by ensuring authenticity and transparency in the ticketing supply chain.

Conclusion

Google's agentic checkout, while heralding a new era of convenience, simultaneously ushers in unprecedented risks for the global sports ticketing supply chain. The amplified capabilities of AI-augmented cybercriminals, particularly through deepfake technology, present a genuine existential threat to the industry's financial integrity and fan trust. Sports properties can no longer afford to be complacent. By embracing a robust Data, AI & Cybersecurity strategy, adopting SASE best practices, and implementing a comprehensive suite of protective measures, the sports industry can transform this challenge into an opportunity to build a more resilient, secure, and trustworthy ticketing ecosystem for the future. The game has changed, and it's time for ‘the defence’ to step up.

[7] Protecting consumers from AI bot ticket and public services hoarding - World ID

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.