# Watermarked.ai Business Plan
# "Securing Authenticity, Protecting Your Digital Audio from Deepfakes"

June 30, 2025

2025 Rice Business Plan Competition.

# Contents


**1 Company summary** **1**

**2 Customer analysis** **1**

**3 Market analysis** **1**

**4 Product or service** **2**

**5 Intellectual property** **3**

**6 Competitive differentiation** **3**

**7 Sales and Marketing Plan** **4**

**8 Company founders and advisor** **5**

**9 Financials** **5**

**10 Amount of investment** **6**

**11 Offering of the company** **6**

**Watermarked.ai** - ***Non-Confidential Executive Summary***

**Website:** www.watermarked.ai **Capital Seeking:** $2 Million USD. **Uses of funding:** Increase sales, marketing and engineering teams along with expansion of computation resources.

---

Product video: `https://youtu.be/7HT3g7t1Iow`

# 1 Company summary

The rise of deepfake content is a growing threat to digital communications, creating challenges for individuals, businesses, and governments. Malicious actors are using any available media to create convincing impersonations in minutes, enabling fraud and misinformation campaigns. Recently, as part of Universal Music Group's negotiations with TikTok, protection from AI-generated deepfakes was a topic of contention [1]. Without proactive measures, these threats will continue to harm revenues, erode trust, and compromise security. Currently, there are no effective preventive measures and the best option is to identify manipulations after they occur. This often requires significant expertise, computational power, and countless man-hours and also cannot undo the damage that the deepfakes cause. The devastating results of the unchecked distribution of deepfakes include monetary and reputational damage to people and organizations.

Our company offers a groundbreaking solution: watermarking technology to embed undetectable signatures into audio files. These watermarks "poison" the content in which they are embedded if used to train deep-fake models, rendering the model ineffective. This proactive approach ensures content authenticity, protects intellectual property, and prevents misuse before it can occur. Our scalable, user-friendly system empowers creators and enterprises to safeguard their audio assets without requiring specialized expertise, helping them thrive in an increasingly AI-driven world.

# 2 Customer analysis

The rise of deepfakes presents a critical challenge to industries reliant on maintaining trust in digital communications, especially musicians, content creators, podcasters, and public officials. Deepfakes pose significant risks to revenue, customer trust, and security.

Current detection tools rely on reactive measures, which are costly, complex, and ill-suited for the fast-evolving threat landscape. Manual reviews and rule-based detection methods are inefficient and fail to scale with the enormous volume of content. Similarly, traditional AI-based detection methods, while effective, remain inaccessible to many due to their high cost, complexity, and reliance on specialized expertise.

In contrast, our watermarking technology offers a proactive solution by embedding undetectable signat ures into audio files to ensure that any misuse, such as using these files to train deepfake models, results in unusable or easily identifiable outputs. This approach addresses the root cause of the deepfake threat by "poisoning" deepfake models attempting to use watermarked content, thus preventing the creation of effective deepfakes.

Through our over 120 customer interviews of stakeholders in music, podcasting, and social media we have found a product like ours fills a gap that these companies are bleeding profit from. The results of these can be seen in Figure 1. Interviewers ranged from executives, sound engineers, copyright analysts, lawyers, producers, Grammy-winning artists, and many more at organizations including Universal Music Group, Warner Music, RIAA, Meta (Instagram), Spotify, and more. Almost all of our interviewers indicated concern with regards to deepfakes and profits, and many believed digital watermarking was the way to go. Additionally, we have demoed our product to many of these stakeholders and are running pilot programs with them.

# 3 Market analysis

IBISWorld analysts project the digital audio protection and content authenticity industry, encompassing deepfake detection and prevention technologies, will see rapid growth in the coming years [2]. The increasing prevalence of audio-based AI applications and the rising threats of deepfake misuse underscore the urgent need for scalable and proactive solutions. Fig. 3 illustrates how this market is expanding, with a focus on serving industries such as entertainment, government, and financial services, where audio authenticity is critical.

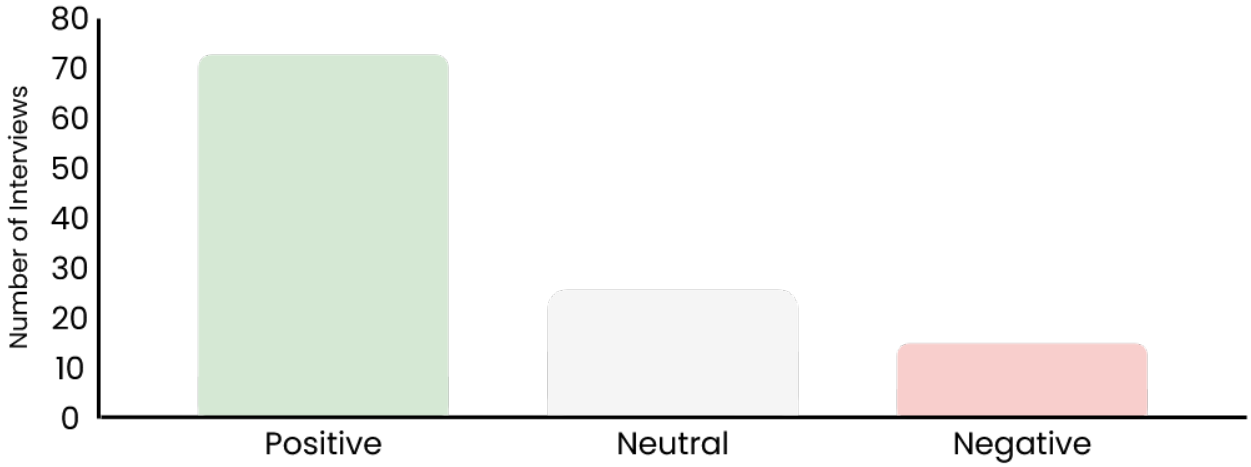


Figure 1: Stakeholders' view on the growing need for a watermark technology to protect digital assets. Interviews were with experts and executives in the audio industry, conducted as part of the NSF I-Corps program in which we received 50k of initial funding.

The Global Digital Content Creation Market was worth 27.1 billion USD in 2023 and projected to be worth 90.4 billion USD by 2033 [3]. The global podcasting market size was estimated to be 25.62 billion USD in 2023 and projected to be worth 135.13 billion USD by 2033 [4]. The global music streaming market was valued at 40.12 billion in 2024 and is projected to grow to 121.43 billion by 2031 [5]. Each of these industries' streaming revenue is under significant threat from deepfakes. From our interviews with various members of these industries, we found revenue loss from deepfakes is a significant and growing threat that executives are worried about and desperately trying to find a solution to.

The market, especially for smaller enterprises, remains underserved. As explained in Section 2, current solutions are manual reviews of content or detection algorithms, which are technically and financially burdensome and not effective against the massive volume of deepfakes. As awareness of deepfake threats grows, IBISWorld's research forecasts smaller content creators, independent businesses, and mid-sized enterprises will be in need of a solution within the next five years [2].

We see a transformative opportunity to meet this strong demand by offering intuitive watermarking tools designed for non-technical users. Our platform simplifies integration into existing workflows, empowering businesses to secure their audio assets without requiring extensive expertise. As the digital audio economy continues to mature and expand, especially with the proliferation of streaming platforms and content-driven enterprises, proactive solutions like ours will become the industry standard.

If we are able to be a service provider to 20% of the current market and assume that about $\sim$1% of all streams are of deepfake content, our service would be able to recover $200 million in lost revenue.

# 4 Product or service

Our innovative deepfake prevention platform eliminates the complexities of safeguarding digital audio, empowering creators, businesses, and enterprises to protect their assets efficiently. By embedding undetectable, tamper-resistant watermarks into digital content, our technology ensures proactive protection against misuse, such as unauthorized deepfake model training. The watermark prevents deepfake models from being able to train on the watermarked content. This allows users to maintain control over their intellectual property while ensuring authenticity in digital communications.

Our watermarking technology has already demonstrated its effectiveness in various scenarios, proving its market demand and technical feasibility. By reducing the complexity of implementing deepfake prevention, we enable content creators and businesses with even a basic technical background to adopt robust audio protection measures quickly. It empowers users to visualize and verify watermark integrity in context, enabling informed decisions to protect their assets. Figure 2 illustrates our platform's competitive advantages compared to current reactive detection tools, in addition to our proactive protection and dataset poisoning.

| FEATURES | WATERMARKED.AI | TRADITIONAL SOLUTIONS | BLOCKCHAIN SOLUTIONS | FINGERPRINTING |
|---|---|---|---|---|
| TAMPERING PROOF | ✓ | ✗ | ✓ | ✗ |
| DEEPFAKE DETECTION | ✓ | ✗ | ✗ | ✗ |
| EASY INTEGRATION | ✓ | ✗ | ✗ | ✓ |
| HIGH VERSATILITY | ✓ | ✗ | ✓ | ✓ |

Figure 2: Current deepfake protection solutions compared to our competitive advantages: proactive prevention, scalability, and tamper-resistant watermarking.

## 5 Intellectual property

Currently, our product is trade secret. Since we have validated our value proposition through numerous customer interviews with stake holders across the audio industry, we are in the process of obtaining patents on our watermarking methodology.

Our IP is safeguarded under a carefully designed licensing structure. While our core system with basic functionalities is available as a test trial, advanced features—including automated watermarking and dataset poisoning—are protected under a GPL v3 license. This ensures that our technology remains accessible for legitimate use while preventing unauthorized commercialization. Our goal is to balance innovation accessibility with the protection of our product's integrity and its rightful usage.

## 6 Competitive differentiation

Our watermarking technology and pilot programs with industry leaders have validated the market need for proactive deepfake prevention, as illustrated in Fig. 1. These collaborations have highlighted a significant gap in the market: the lack of accessible, scalable, and proactive solutions tailored to organizations with limited technical resources. The table below provides a comparative analysis of Watermarked.ai and its key competitors in the digital audio watermarking, intellectual property protection, and deepfake prevention sectors. It highlights each company's solution technology approach, strengths, and limitations. This structured overview emphasizes how Watermarked.ai distinguishes itself through its proactive watermarking technology designed to sabotage deepfake training pipelines, addressing critical gaps in the market that competitors have yet to fully address. By analyzing the strengths and limitations of existing solutions, this table offers insights into potential opportunities for Watermarked.ai to establish a unique market position.

In contrast to indirect competitors, such as open-source AI frameworks like Keras and TensorFlow, which require specialized AI development teams to build custom solutions, our platform provides a ready-to-use, intuitive solution designed for non-technical users. This eliminates the high costs and complexities of staffing and development, making our technology highly appealing to organizations seeking efficient, scalable tools. Our focus on usability and ease of deployment empowers teams to adopt deepfake prevention measures effectively, bypassing the barriers associated with traditional AI-driven detection or watermarking solutions.

To validate these competitive advantages, our team has conducted successful pilot programs with leading companies in the media, technology, and government sectors, as highlighted in Fig. 2. These pilots confirmed the scalability, reliability, and practical applications of our technology in proactively addressing deepfake threats. By embedding tamper-resistant watermarks into digital content, we offer a robust and scalable approach to deepfake prevention that has garnered recognition from stakeholders seeking user-friendly tools to combat the growing risks of deepfake audio and video. Our commitment to proactive protection, usability, and scalability positions us as a leader in the fight against deepfake misuse.

| Company | Solution Technology Approach | Strengths | Limitations |
|---|---|---|---|
| Amazon Science | Real-time spread-spectrum modulation with autocorrelation-based synchronization | Low computational complexity, resilient to ambient noise and reverberation | Focused on echo cancellation (not deepfake prevention), limited to Alexa ecosystem integrations |
| Audible Magic | Hybrid fingerprinting + Activated Content's imperceptible watermarks for forensic tracing | Industry-standard anti-piracy database, scalable for large content libraries | Relies on partnerships for watermarking tech, no proactive deepfake disruption |
| Pindrop | AI-driven voice authentication + watermarking analysis for telephony channels | Optimized for voice call degradation (e.g., packet loss), multi-layer security | Watermarking secondary to detection, tradeoffs between audio quality and security |
| SourceAudio | High-fidelity watermarking integrated with digital asset management systems | DAW-compatible detection, royalty tracking for music/broadcast | Vulnerable to re-recording attacks, limited persistence in edited audio |
| Activated Content | Tamper-evident watermarks robust to MP3 compression and format conversion | Legal-grade evidence for piracy cases, pre-release leak prevention | No active product presence (historical tech), lacks AI-specific applications |
| Watermarked.ai | Proactive imperceptible watermarks designed to corrupt deepfake model training datasets | Sabotages AI training pipelines, universal applicability across audio formats | New entrant. Lower market recognition |

Table 1: Comparative Analysis of Competitors in Digital Audio Watermarking and Deepfake Prevention

# 7 Sales and Marketing Plan

Our comprehensive research, supported by extensive customer interviews and successful pilot programs, has allowed us to align our watermarking technology precisely with the needs of digital content creators and enterprises, enhancing the attractiveness of our solution to both customers and private investors. The commercialization strategy detailed here directly addresses the challenges identified through our continuous customer discovery process.

Watermarked.ai's go-to-market strategy involves embedding our proprietary watermarking solution directly into digital content workflows via strategic partnerships, direct sales, and licensing agreements. We plan to deploy a dedicated sales team experienced in enterprise software solutions, utilizing strategic alliances with influential industry players, including the Recording Industry Association of America (RIAA) and the International Federation of the Phonographic Industry (IFPI), both of whom have expressed strong interest and provided positive feedback on our pilot tests.

Our SaaS business model will generate revenue through initial setup fees for infrastructure integration and ongoing subscription charges based on data volume processed and premium features. Strategic partnerships with key industry players such as SaaS providers, cybersecurity firms, and content management platforms, including Fortune 500 companies, will facilitate rapid adoption and accelerate market penetration.

To maximize visibility and credibility, Watermarked.ai will conduct comprehensive content marketing initiatives, such as informative blog articles, detailed whitepapers, case studies, industry reports, and compelling explainer videos. Active participation in leading industry conferences, webinars, and targeted digital marketing campaigns will further amplify our presence and authority in the field of digital asset protection.

Customer engagement and retention strategies include showcasing tangible outcomes from successful pilot programs, providing extensive onboarding support, and establishing dedicated customer success teams to deliver ongoing training and support. By continuously refining our offerings based on client feedback, we aim to build lasting relationships, driving high customer retention rates and facilitating growth through referrals

and expanded adoption.

# 8 Company founders and advisor

Watermarked is a young startup established in 2024 with its origins in the AI research community. Our team brings together the technical expertise with validated AI experience and the entrepreneurial skills to materialize our vision into a business reality. We are planning additional key hires that involve an experienced operations officer and expanding our programmer workforce.

**Bikrant Das Sharma** is a Ph.D. student at the University of Illinois, Urbana-Champaign studying Computer Science. He completed his undergraduate degree at Rice University in May of 2024. Bikrant has been involved with Watermarked since its start. He went through the NSF's I-Corps entrepreneurial training program, where he conducted over 120 customer interviews to understand the problems the audio industry is encountering and what solutions they are looking for. Bikrant's background with the startup ThousandEyes—acquired by Cisco Systems—provided him with a unique insight into the dynamics of running a successful tech startup, from understanding the team structures to mastering the workflow processes that drive growth. This experience, coupled with his extensive Silicon Valley network, positions him as a key connector between the research lab and potential industry partners, investors, and technology leaders.

**Leroy Souz** is an undergraduate student at Rutgers University pursuing a double major in Computer Science and Data Science. He is currently working with Dr. Ruixiang Tang on enhancing the trustability of Large Language Models. He has worked on various projects aimed at enhancing the safety of AI models, including developing tools to detect and mitigate risks in AI systems and testing new safety protocols. Leroy is also an excellent public speaker and mentor, having successfully guided over 20 students in his machine learning club to build models from scratch, despite their initial lack of ML expertise. His ability to communicate complex technical concepts clearly and effectively, combined with his leadership skills, makes him a valuable asset in pitching ideas and collaborating with diverse stakeholders.

**Advisor, Ruixiang (Ryan) Tang** is an Assistant Professor at Rutgers University with expertise in artificial intelligence, machine learning, and multimedia security. He earned his Ph.D. in Computer Science from Rice University, where his research focused on advancing trustworthy AI methodologies. Dr. Tang has extensive experience in developing watermarking techniques across various domains, including audio, text, and images. His work addresses critical challenges in protecting intellectual property, ensuring the integrity of AI-generated content, and enhancing transparency in machine learning systems. Dr. Tang has contributed to cutting-edge research on robust and imperceptible watermarking methods, with applications spanning digital media authentication, AI model protection, and content provenance tracking. Through his work, he aims to bridge the gap between theoretical advancements and real-world applications, collaborating with academia and industry to create innovative solutions for secure and ethical AI deployment.

# 9 Financials

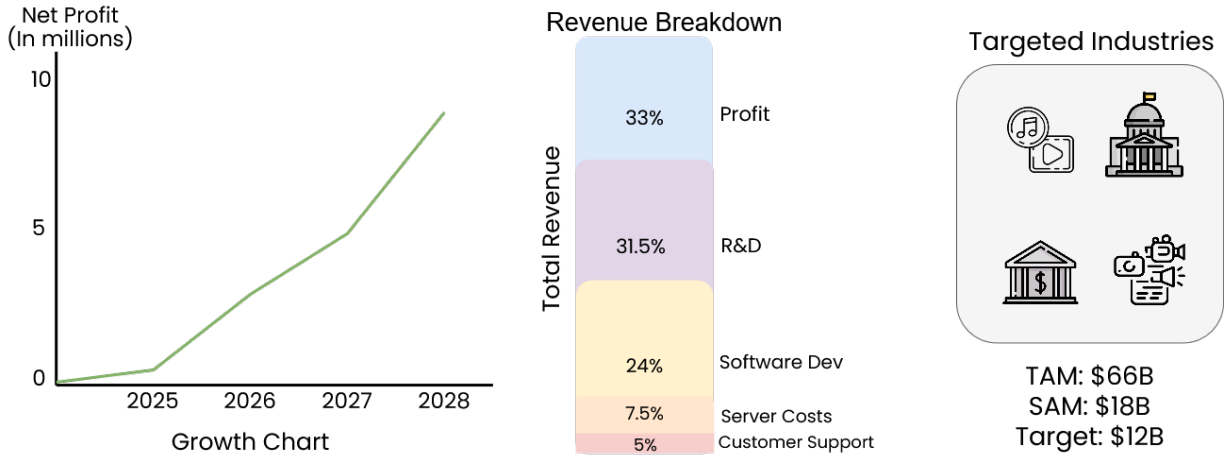


Figure 3: Projected growth and breakdown of the digital audio protection market.

Our watermarking technology has gained significant traction through pilot programs with industry leaders, proving its effectiveness in addressing deepfake threats. These pilot initiatives have become a cornerstone of our marketing and validation strategy, enabling us to showcase real-world applications and build strong relationships with key stakeholders. Collaborations with industry partners have not only helped refine our technology but also resulted in early adoption by paying customers, underscoring the value of our solution in high-risk environments.

Early adopters have requested customized features like advanced watermarking, real-time monitoring, and system integration. We work closely with clients to co-develop solutions that meet their specific needs. Our fundraising plan focuses on expanding these pilots and scaling outreach to new industries through direct partnerships, showcasing the scalability, reliability, and value of our technology. This approach positions us to build long-term customer relations while accelerating adoption and establishing a leading position in the deepfake prevention market.

Our business model includes both non-recurring revenue and recurring revenue. Non-recurring revenue streams include setup costs, such as watermark customization, platform installation, training, deployment support, and data integration services. Recurring revenue streams are modeled on successful SaaS platforms, like AWS®, and include subscription fees for ongoing watermarking services, data volume processed, and premium features such as advanced analytics, tamper detection, and enterprise-grade security options. With an expected SaaS margin of 80-85%, we anticipate a $21,000 monthly burn rate in the first year of scaling operations.

We aim to expand our customer base, focusing on enterprises vulnerable to deepfake threats. Through pilot programs with key industry players, we are continually improving our intuitive watermarking solution to address diverse use cases, including fraud prevention, content authentication, and compliance with digital rights management standards. Partnerships with companies like Amazon and LinkedIn highlight the potential for growth and wider adoption.

| Financials ($0 US) | 2024 | 2025 (projected) | 2026 (projected) | 2027 (projected) | 2028 (projected) |
|---|---|---|---|---|---|
| Revenue | 50k | 1.3M | 7M | 10M | 15M |
| Expenditures | 30k | 900k | 4M | 5M | 7M |
| Net | 20k | 400k | 3M | 5M | 8M |

Table 2: Projected financials of watermarked.ai over a 5 year period from 2024 to 2028.

# 10 Amount of investment

Our central motivation to participate at the Rice Business Competition is, first and foremost, **to find mentoring that can help us refine our SaaS-focused business model**. Equally important is to raise our Seed round of $2 million. We will allocate the investment to grow our team and expand our Automatic Data Processing Equipment capabilities and better serve our current users and customers.

It is essential to highlight that we have formed a team to commercialize our technology, and are submitting an SBIR application. Our team will designate any potential non-dilutive funding to move forward our internal research and technology commercialization agenda.

Our technology has already generated substantial interest, with pilot programs validating its commercial viability. Although we are in the early stages of monetization, we anticipate rapid revenue growth as we expand adoption and scale operations.

# 11 Offering of the company

Watermarked.ai is seeking an investment of $2 million USD to accelerate the commercialization and expansion of our proactive watermarking solution designed to combat audio deepfake threats. This funding will primarily be utilized to scale our sales and marketing capabilities, expand our engineering and technical teams, and enhance our computational infrastructure to support growing customer demand.

Specifically, the investment will enable us to significantly strengthen our direct sales initiatives and marketing outreach, facilitating broader adoption across targeted industries, including music, podcasting, social media, and government agencies. Additional resources will support the refinement of our product features,

further enhancing automation, scalability, and ease of integration, ensuring we meet the evolving demands of the digital content protection market.

We anticipate multiple exit opportunities for investors, including strategic acquisition by major cybersecurity firms, SaaS providers, or leading media and technology companies actively expanding their digital protection offerings. Alternatively, as the business grows, an IPO could present a viable exit strategy, particularly if our technology achieves widespread adoption and establishes market leadership within the rapidly expanding audio content authenticity and protection industry.

# References


[1] Ben Sisario. *Universal Music Group Pulls Songs from TikTok*, February 1, 2024. https://www.nytimes.com/2024/02/01/arts/music/universal-group-tiktok-music.html.

[2] Jared Ristoff. *Intellectual Property Licensing in the US - Market Research Report (2014-2029)*, March 2024. https://www.ibisworld.com/united-states/industry/intellectual-property-licensing/1385/.

[3] market.us. *Global Digital Content Creation Market Size, Share Report By Component (Tools and Services), By Deployment Mode (Cloud-Based and On-Premise), By Content Type (Video, Textual, Graphical, and Audio), By Enterprise Size (Small Medium Enterprises and Large Enterprises), By End-Use Industry (Retail E-Commerce, Automotive, Healthcare Pharmaceutical, Media Entertainment, Travel Tourism, Other End-Users), By Region and Companies - Industry Segment Outlook, Market Assessment, Competition Scenario, Trends, and Forecast 2024-2033*, October 2024. https://market.us/report/digital-content-creation-market/.

[4] Coherent Market Insights. *Podcasting Market Analysis*, June 2024. https://www.coherentmarketinsights.com/market-insight/podcasting-market-4283.

[5] Coherent Market Insights. *Music Streaming Market Size and Share Analysis - Growth Trends and Forecasts (2024-2031)*, December 2024. https://www.coherentmarketinsights.com/industry-reports/music-streaming-market.