



✓RealityChek

Adaptive **Cybersecurity Solutions** for the Age of AI

✓RealityChek.com

WELCOME TO

The **Cybersecurity** **Solution** Securing Reality in the Age of AI

✓RealityChek

OUR MISSION AND VISION

A functioning society depends on a reality that is secure, trusted, and verifiable.

In an age where artificial intelligence can fabricate images, videos, and written content with alarming precision, distinguishing reality from deception has become increasingly difficult —**and critically important for the world.**

Founded by tech entrepreneurs and AI-visionaries, **RealityChek** is a cutting-edge **cybersecurity solution** designed to detect AI-generated content and safeguard the integrity of authentic information. **Whether it's manipulated images, deepfake videos, or AI-authored text, we are building proprietary algorithms and forensic tools provide fast, reliable detection to help organizations, institutions, and the public separate fact from fabrication.**



\$485 Billion

Global Cybersecurity Opportunity

The problem is massive and expanding rapidly as AI-driven fraud accelerates across industries, posing a major threat to enterprises and government. **With fraud losses in U.S. alone projected to hit \$40 billion by 2030, and 46% of businesses already targeted by identity fraud driven by deepfakes, the risks are escalating fast.** Deepfake incidents alone surged 245% globally in 2024.

\$250

Billion Dollar Market 2025

14%

CAGR 2025-2030

\$485

Billion Dollar Market 2030

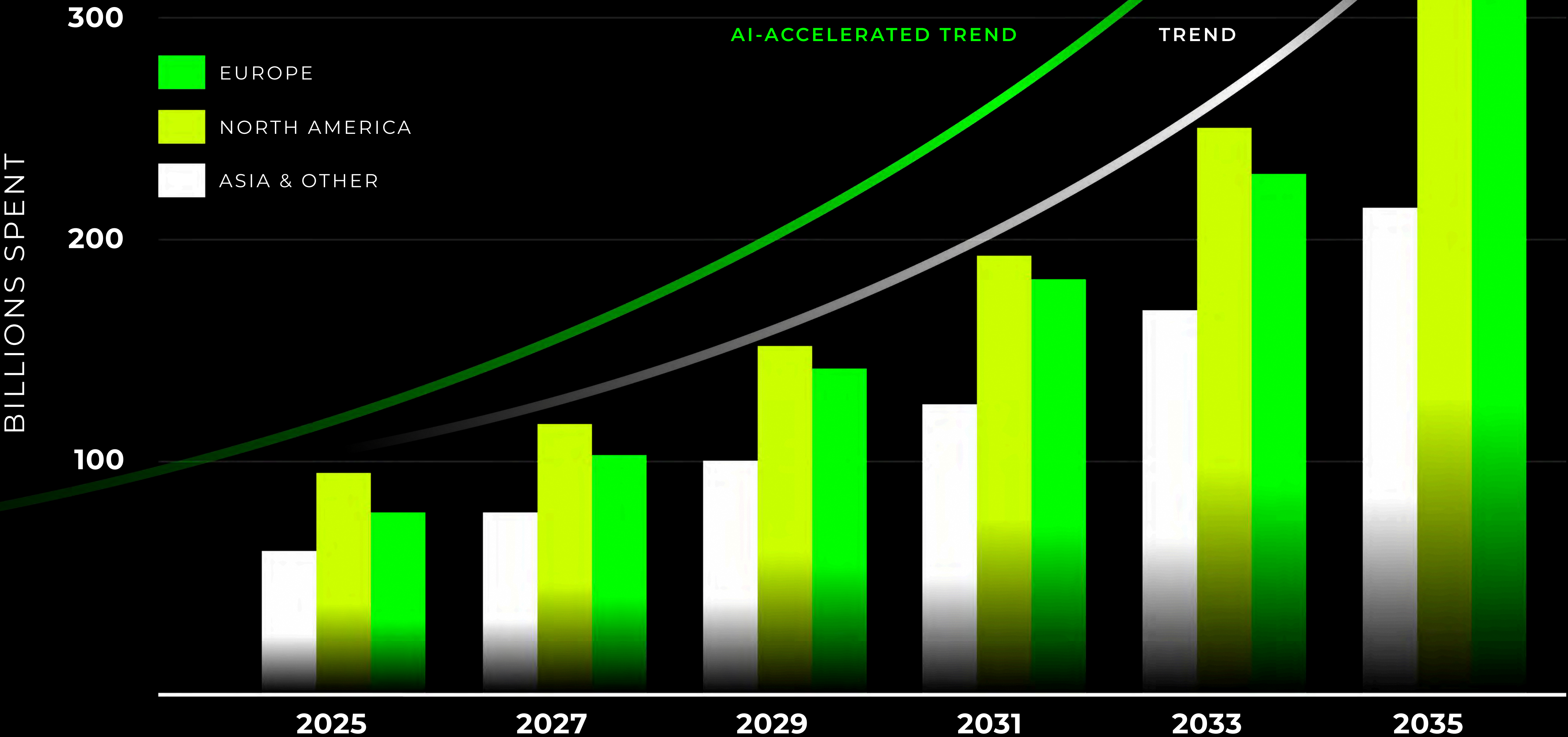
EST \$250B IN 2025 WITH CAGR 14%. FIGURES IN USD. SEE SOURCES AT END.

Global **Cybersecurity** Opportunity

FORECAST BY REGION (2025-2035)

EST FIGURES IN USD. SEE SOURCES AT END

RealityChek



THE SOLUTION WE ARE BUILDING



At the core of the system is an advanced AI detection engine built on a multidimensional forensic framework.

Rather than relying on a single model, **RealityChek continuously evaluates and stress-tests the most advanced forensic methodologies available.** Through a sophisticated benchmarking environment, we rigorously test detection techniques against evolving synthetic content across text, image, audio, and video.

For each media type, we implement the highest-performing models and detection strategies based on measurable accuracy, resilience, and adversarial robustness. This layered, media-specific approach ensures that the system adapts as generative AI evolves, maintaining best-in-class performance rather than static capabilities.

Developed by world-class experts in AI and cybersecurity, **RealityChek is engineered to equip corporations, institutions, and individuals with scalable, real-time tools to identify, flag, and verify synthetic or misleading digital content instantly.** In an era where deepfakes and manipulated information spread faster than facts, RealityChek is built to protect reputations, reinforce trust, and preserve the integrity of digital interactions and transactions.

A NEW REALITY
AI-Driven Deception Types

False Connection

Headlines, visuals, or captions don't support the content.



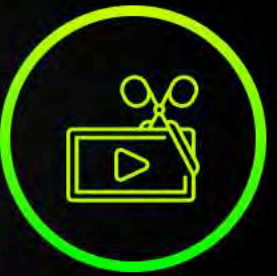
False Context

Genuine content is shared with false contextual information.



Manipulated Content

Genuine information or imagery is manipulated to deceive.



Satire or Parody

No intention to cause harm, but can still fool people.



Misleading Content

Misleading use of information to frame an issue or individual.



Sponsored Content

Advertising or press releases disguised as editorial content.



Imposter Content

Genuine sources are impersonated.



Error

Mistakes made by established news organizations while reporting.



Propaganda

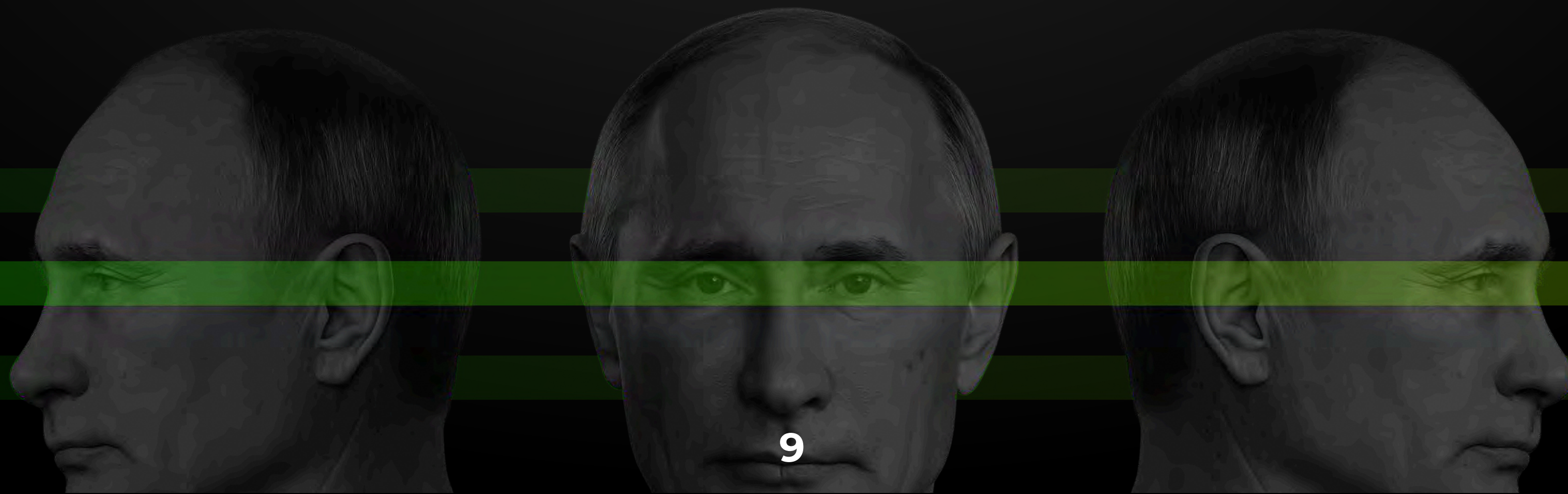
Content used to manipulate attitudes, values, and knowledge.



What is a deepfake?

A deepfake is AI-generated video, audio, or imagery engineered to convincingly replicate a real person, scene, voice, or document. It can be entirely synthetic or a manipulated version of authentic content. While some deepfakes are created for entertainment or artistic experimentation, many are designed to deceive, distort reality, or exploit trust.

As generative AI continues to evolve at an exponential pace, these fabrications are becoming increasingly sophisticated—blurring the line between what is real and what is artificially constructed. We are rapidly approaching a point of no return, where reality and fiction may become indistinguishable to the human eye and ear. **In that world, trust can no longer rely on perception alone. Society will be forced to evolve—developing new verification standards, detection systems, and digital literacy frameworks—to preserve truth in an era where seeing is no longer believing.**





Can you spot the imposter?

All of these are AI-generated. The line separating reality from fabrication is dissolving at an exponential pace, creating a world where identities, voices, documents, and even events can be convincingly manufactured. As synthetic media scales, the question is no longer whether manipulation is possible — it's how we protect what's real.

How will governments authenticate citizenship applications, passports, and official identification?

How will institutions defend against AI-crafted news and video engineered to distort perception and influence elections?

In an era of digital uncertainty, securing truth itself becomes a matter of security.

REAL WORLD EXAMPLE



Passport Document Manipulation

ALTERED IMAGE

AI TEXT

• ALTERED PIXELS

• ALTERED IMAGE

[illegible]

Government Broadcast

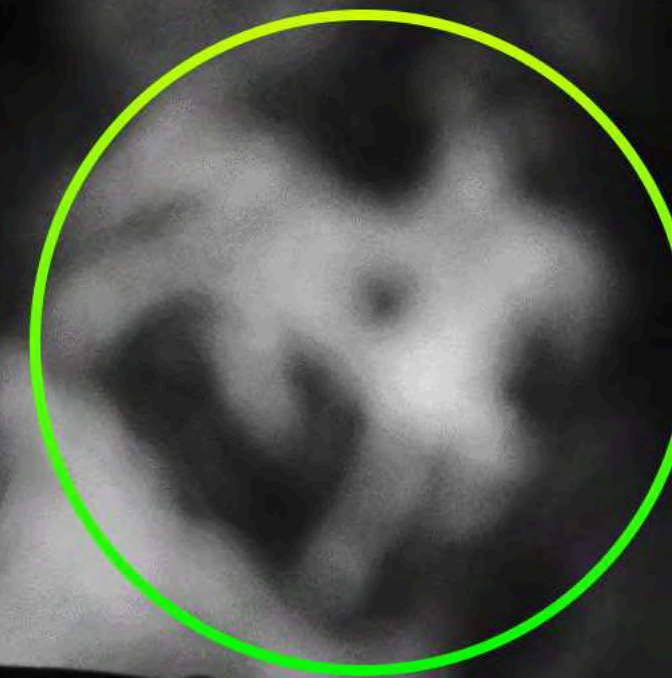
ALTERED PIXELS



FACIAL
INCONSISTENCIES



NOISE AND TEXTURE
INCONSISTENCIES



RENDERING ERROR





Our tech detects and analyzes data across multiple modalities and media types, delivering an advanced security layer that secures digital interactions and transactions.

For each media type, we deploy the highest-performing models and detection strategies based on measurable accuracy, resilience, and adversarial robustness. This layered, media-specific architecture continuously adapts as generative AI evolves—**ensuring best-in-class performance rather than static, outdated defences.**

Constant Model Evolution

We are building a system that will continuously ingest AI-generated content across text, image, audio, and video from public and proprietary sources. **Our models will be updated daily to stay ahead of rapidly evolving synthetic threats.**

Advanced Detection Engine

At the core, we are developing a multidimensional AI forensic engine. **We will continuously benchmark and stress-test advanced detection methodologies, implementing the highest-performing models for each media type based on measurable accuracy and resilience.**

Adversarial Learning

Our architecture will use AI to detect AI. **Through adversarial training techniques, detection models will be hardened against increasingly realistic synthetic content, improving as generative systems evolve.**

Multimodal Detection

We are building a layered detection framework that will analyze content through multiple signals and contextual indicators to maximize accuracy while minimizing false positives.

Scalable, Secure Infrastructure

RealityChek is being engineered as a secure, **high-performance API** designed to integrate into enterprise platforms, financial systems, media networks, and government infrastructure.

Explainable & Audit-Ready Results

For enterprise and legal-grade clients, we will provide transparent detection scores and structured reporting designed to **meet compliance, audit, and evidentiary standards.**

REQUEST API OR APPLICATION

A user submits content—video, text, or audio—through the application or API. The system intelligently routes the request, aligning the appropriate detection tools and media-specific models. The content is then analyzed by our AI core engine, where it is processed through multiple layers of forensic methodologies, models, and validation tools to assess authenticity and integrity.

EXAMPLE:

*LEASE DOCUMENT WITH
IDENTITY IMAGES IS SUBMITTED
VIA AUTOMATION SOFTWARE (API)*



CORE DETECTION ENGINE

RETURN REALITY COEFFICIENT

Once the request has been processed by the core detection engine, it returns a structured data array that includes a Reality Coefficient—ranging from 0 (entirely synthetic) to 1 (fully authentic). Depending on the user's requirements, the response can also include hundreds of additional forensic and analytical data points to support deeper validation and decision-making.

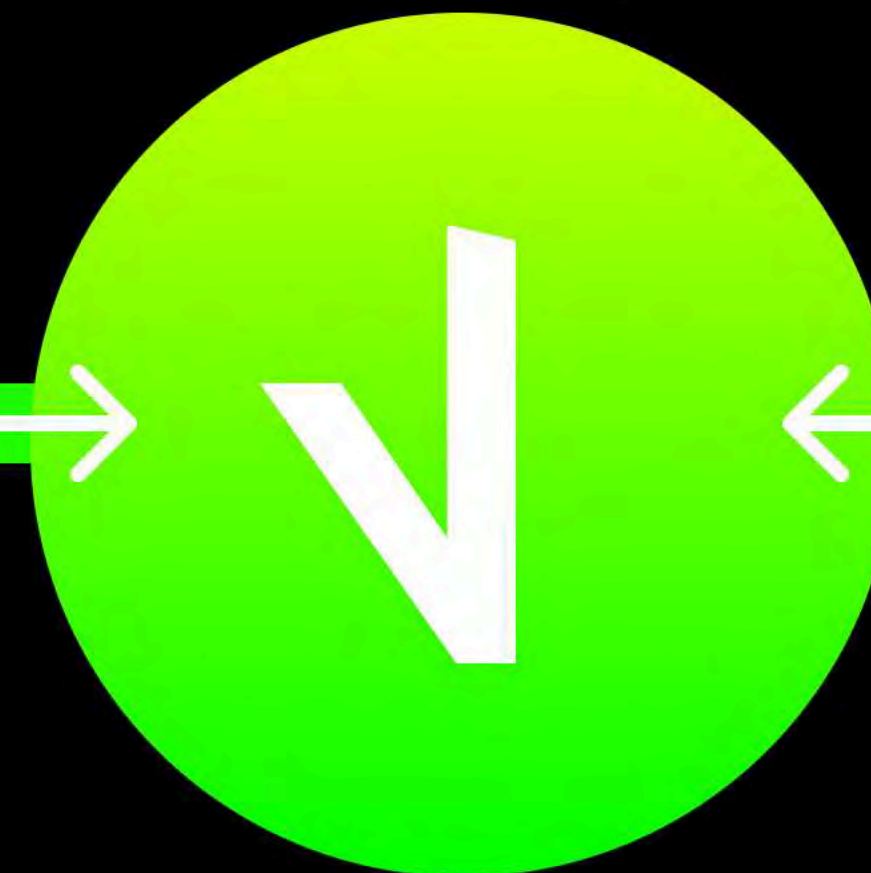
EXAMPLE:

*SET BY THE USER, THE LEASE
DOCUMENT PASSED A 0.95 REALITY
COEFFICIENT AND CAN GET
PROCESSED BY NEXT WORKFLOW*

Our planned model is comprised of the best-performing detection models, advanced techniques, and forensic methodologies available, all selected through a sophisticated benchmarking and stress-testing framework. Rather than relying on a single approach, we continuously evaluate and compare open-source, proprietary, and internally developed systems across multiple media types, measuring accuracy, resilience, and adversarial robustness. Only the highest-performing models and techniques are integrated into the core engine, ensuring that **RealityChek** remains adaptive, data-driven, and built on measurable performance rather than static assumptions.

INTERNAL OR ACQUIRED MODELS AND TOOLS

- Continuous adversarial training (AI vs AI red teaming)
- Ensemble meta-classifier with dynamic weighting
- Zero-day anomaly detection models
- Frequency domain forensic analysis (FFT/DCT artifact detection)
- Sensor pattern noise (camera authenticity verification)
- Pixel-level residual & diffusion artifact detection
- Frame-level temporal inconsistency modeling (video)
- Spectral & phase coherence modeling (audio deepfake detection)
- Cross-modal consistency verification (voice-lip-text alignment)



CORE DETECTION ENGINE

3RD PARTY, OPEN SOURCE MODELS AND TOOLS

- Identity embedding fusion (face + voice + behavioral vectors)
- Stylometric authorship & LLM fingerprinting
- AI watermark detection (multi-model watermark scanning)
- Reverse generative model attribution
- Large-scale multimodal transformer anomaly detection
- Metadata integrity & provenance analysis
- EXIF validation & manipulation detection
- Model drift detection with automatic retraining triggers
- Confidence calibration & probabilistic consensus scoring

GAMIFIED DATA-LABELLING TO STRENGTHEN OUR MODEL

REAL



FAKE

The Reality Games are blockchain-based play-to-earn games designed to strengthen and evolve advanced AI-detection models. Much like how Google's reCAPTCHA trained image-recognition systems by engaging users in micro-tasks, The Reality Games leverage player interactions and rewards to continuously improve the accuracy, intelligence, and resilience of our Security Models.

TARGETED
MARKETING

GAMIFIED
DATA LABELING

MODEL
EFFECTIVENESS
IMPROVED

RealityChek already holds 5 million+ datapoints and 2 million+ assets
— stored and labeled.

As we grow, we are building one of the world's largest labeled datasets—with access to over **3+ billion assets**—designed to continuously optimize and harden our AI reality models.

We are continuously testing and integrating new models, pushing us closer to achieving truly reliable, near-100% threat detection.



Cybersecurity

Solutions that detect AI-driven fraud, deepfakes, and manipulated content.

Driven by SaaS subscriptions, API licensing, and usage-based fees for organizations integrating verification and authentication layer into their security infrastructure.



Data Labeling

High-integrity, human-validated datasets used to train AI detection and fraud-prevention models.

Revenue comes from data licensing, subscriptions, and custom dataset creation for AI companies, governments, and cybersecurity firms.

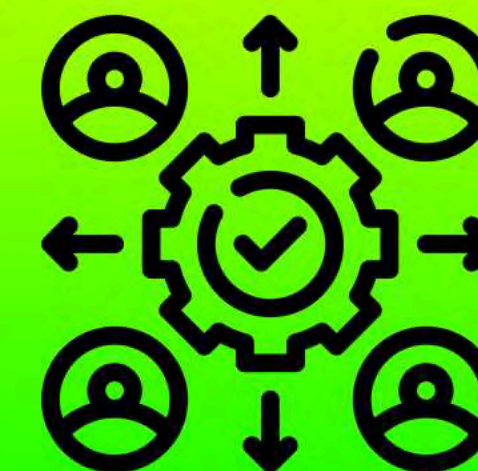
Our goal is to become the most advanced cybersecurity solution for the AI era — delivering near-perfect fraud prevention while preserving trust in every transaction.

0-6 Months

- Alpha Testing
- Dashboard Prototype
- Core Architecture Framework
- Team Development

6-12 Months

- Beta Launch
- API Framework
- Features Onboarding
- Cloud & Data Framework
- Testing & Optimization
- Model Acquisitions
- Team Development

12-24 Months

- API Launch
- Model Hardening
- Core Tech Launch
- Scale Optimization
- Automation Integration
- Feedback Implementations
- Team Development

Karl Kottmeier - Chief Executive Officer

Karl has over 25 years of experience in venture capital corporate finance, having created and developed numerous companies from inception through to successful listing on the TSX, TSX Venture, and CSE Exchanges where he raised in excess of **\$250,000,000 for public companies**. Prior to his career in private and public company corporate finance and administration, Karl was in retail brokerage **focusing on venture capital for 10 years**.

Chris Vassos - Chief Technology Officer

Chris has held various positions in the technology industry, including system designer, software programmer and system manager/engineer. He currently manages Hydaway's rendering operations, having designed, sourced and constructed the computer system that powers the company's operations. Mr. Vassos has 4 years' experience in Linux programming, **5 years as a Linux system administrator and 10 years' experience in computer system/data architecture design and construction, crypto mining and information technology**.

Natasha Tsai - CPA, CA - Chief Financial Officer

Natasha brings extensive experience as Managing Director at Malaspina Consultants Inc. **She has been a senior advisor and CFO with companies in a broad range of industries**, and specializes in the areas of financial operations and business performance. A graduate of UBC Sauder School of Business, Tsai received her Chartered Accountant designation in 2007 and has served as co-chair of the Young CA Forum at the Institute of Chartered Accountants of BC.

Amin N. - Chief Product Officer

Amin is a technology entrepreneur with over 20 years of experience building and scaling companies, including publicly listed ventures. He transforms ambitious ideas into high-growth businesses by aligning product innovation with disciplined execution. He has scaled products to six-figure MRR and platforms serving hundreds of thousands of users, with a focus on long-term impact and scalability.

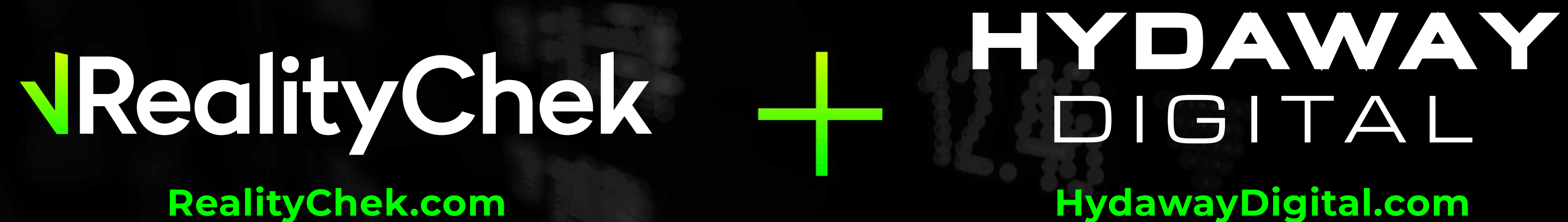
Ethan J. - Chief Product Engineer

Ethan is a developer and venture builder with over 5 years of experience building AI and SaaS products that turn ambitious ideas into scalable platforms. He architects high-performance web applications, automation systems, and AI integrations from concept to deployment, leveraging modern tools like Replit. Focused on clean architecture and scalability, he combines technical execution with product vision to build powerful, design-driven solutions.

Matthew S. - Chief Marketing Officer

Matthew is a technology entrepreneur and marketing strategist working at the intersection of capital markets, media, and emerging technologies. With a background in building web applications and advanced marketing funnels, he specializes in developing scalable digital platforms that integrate content, video, automation, and data-driven strategy to generate meaningful engagement for public companies. Known for his forward-thinking approach, he leverages AI, digital infrastructure, and strategic storytelling to strengthen brand positioning and drive measurable growth.

PUBLICLY TRADED



RealityChek went public through acquisition by Hydaway Digital Corp., providing an efficient pathway to the public markets while preserving capital for growth. The transaction consolidated the company's technology, intellectual property, and leadership under the publicly listed entity, **positioning RealityChek to accelerate development and expand investor access as it builds the next generation of AI-driven authenticity and cybersecurity infrastructure.**

TSXV:**HIDE**

CAPITALIZATION TABLE

Shares Outstanding	37,542,713
Warrants	4,800,000
Options	2,350,000
FULLY DILUTED SHARES	44,692,713

The company maintains a tight and controlled capital structure. Vendors hold approximately 16% with additional performance-based earnout alignment, reinforcing long-term commitment. Warrants are priced at \$0.40, linking dilution to upside, with approximately \$2.3M in potential cash upon exercise. The company has a clean public structure built for growth.

FINAL NOTE

RealityChek was founded on a simple but urgent belief: if reality cannot be trusted, nothing else can. As artificial intelligence accelerates and synthetic content becomes indistinguishable from authentic human expression, society is approaching a turning point. Identity, financial systems, elections, journalism, contracts, and even personal relationships depend on a shared understanding of what is real. Without a mechanism to preserve that trust, the digital foundation of modern civilization begins to erode.

Our mission is to preserve reality in an AI-driven world. We envision a future where truth is not left to chance, where verification is embedded into global systems, and where individuals, corporations, and governments can operate with confidence in the integrity of digital information. RealityChek is driven by the conviction that technological progress must be matched with technological accountability — that as AI grows more powerful, so must the safeguards that protect humanity.

We are building toward a world where trust is engineered, identity is protected, and authenticity becomes a standard — not a luxury. RealityChek exists to ensure that as AI reshapes the world, truth remains intact.

A wide-angle landscape photograph featuring a dark sand beach in the foreground, dotted with green coastal vegetation. In the background, rugged mountains rise against a sky filled with large, white and orange-tinted clouds, suggesting a sunrise or sunset. The overall scene is serene and majestic.

✓RealityChek

Securing Reality in a Synthetic World.
Thank you for reading.

✓RealityChek.com

SOURCES

<https://www.cheq.ai/blog/the-economic-cost-of-bad-actors-on-the-internet>
<https://cepr.org/voxeu/columns/buzz-bust-how-fake-news-shapes-business-cycle>
<https://www.uni-bonn.de/en/news/134-2024>
<https://www.entrust.com/cybersecurity-institute/podcasts/disinformation-cost>
<https://www.linkedin.com/pulse/fake-news-factory-78-billion-threat-nations-trust-sanjay-mxhxf>
<https://www.hkubs.hku.hk/research/thought-leadership/hkej-column/combat-misinformation-for-a-stable-economy>
<https://www.pewresearch.org/journalism/fact-sheet/news-platform-fact-sheet/>
<https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/>
<https://www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2022055-eng.htm>
<https://www.emarketer.com/content/canada-time-spent-with-media-2024>
<https://www.marketsandmarkets.com/Market-Reports/deepfake-detection-market-111124063.html>
<https://www.alliedmarketresearch.com/deepfake-detection-market-A16917>
<https://www.statista.com/outlook/tmo/cybersecurity/worldwide>
<https://www.grandviewresearch.com/industry-analysis/ai-in-media-entertainment-market>
<https://www.grandviewresearch.com/industry-analysis/identity-verification-market>
<https://www.marketsandmarkets.com/Market-Reports/fraud-detection-prevention-market-1311.html>
<https://www.fortunebusinessinsights.com/defense-it-spending-market-105030>
<https://artificialintelligenceact.eu/>
<https://www.congress.gov/bill/117th-congress/house-bill/2395/text>