CYBERSECURITY

# WHITE PAPER

We are Experts at Engaging Experts

**HITECH ADVISORS**

www.hitechadvisors.com | hello@hitechadvisors.com | (425) 284-3315

HITECH ADVISORS

# Deepfakes and the Rising Cybersecurity Threat to Insurance

Deepfake technology—synthetic media created using AI—has emerged as a powerful new vector for fraud and reputational harm in the insurance industry. Criminals are using convincingly fake audio, video, and documentation to exploit digital workflows, manipulate claims, impersonate agents, and fabricate identities. As trust remains a foundational pillar of insurance, these synthetic threats now pose not just technical risks but regulatory, financial, and reputational ones as well.

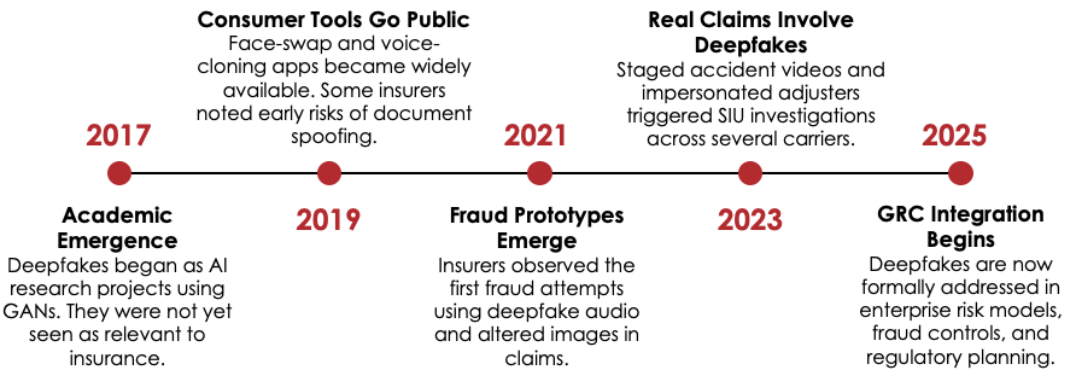
> “Deepfakes are reshaping fraud—and insurance must respond with digital vigilance, not denial.”

This white paper explores how deepfakes are impacting the insurance sector, with real-world examples, detection strategies, and a roadmap for leadership action. From claims fraud to social engineering, the paper offers a tactical and strategic lens on defending policyholder trust in an era where seeing and hearing is no longer believing.

## Understanding Deepfakes in the Insurance Context

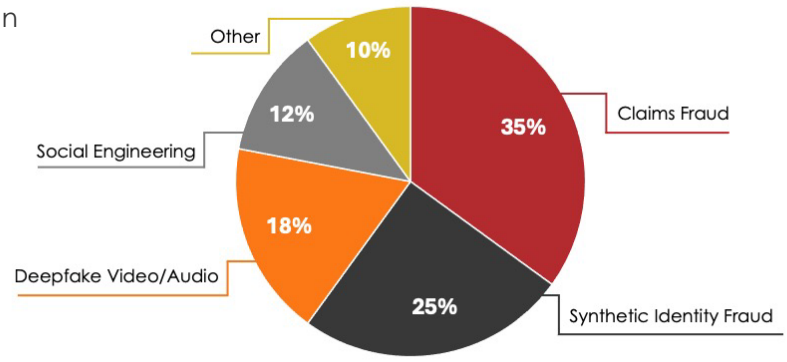
Deepfakes are AI-generated media—audio, video, images, or documents—that mimic real individuals or scenarios. Fueled by advances in generative adversarial networks (GANs), these forgeries are now sophisticated enough to pass as authentic across digital channels. In insurance, this introduces new risks at multiple touchpoints—from claim submissions and policy onboarding to internal communication and public trust.

Initially seen in entertainment or politics, deepfakes are rapidly being weaponized in commercial fraud schemes. Their realism and accessibility have exploded. Pre-trained models and deepfake-as-a-service offerings on the dark web make them available to low-skill attackers and organized crime alike. The insurance industry’s growing reliance on remote verification, video documentation, and digital claims processing creates ideal conditions for exploitation.



# Threat Landscape for Insurers

The insurance industry sits at the intersection of high-value transactions, personal data, and trust—making it an attractive target for synthetic media threats. As deepfakes become more realistic, affordable, and accessible, fraudsters are using them to exploit common workflows like claims processing, customer onboarding, and policyholder communication. Unlike traditional fraud, deepfakes bypass static defenses by mimicking trusted people, documents, and interactions. This section explores the key vectors where deepfakes are already being used—or soon will be—to disrupt, deceive, and defraud insurers across lines of business.




### Claims Fraud

Deepfakes are increasingly used to falsify documentation during the claims process. Examples include AI-generated video footage of staged accidents, doctored damage photos, and voice impersonations of policyholders authorizing claim payouts. These tactics can slip past traditional fraud filters, delaying legitimate claims and costing millions in improper disbursements.

### Synthetic Identity Onboarding

Fraud rings are using synthetic personas—constructed with AI-generated images, documents, and audio—to open policies and launder money through fake premium payments and fraudulent payouts. Deepfakes can defeat KYC systems and video verification steps that insurers rely on.

### Agent & Adjuster Impersonation

Bad actors are now creating deepfaked calls or video messages impersonating trusted agents or adjusters. These impersonations can be used to redirect payouts, collect sensitive data, or deceive policyholders during high-stress events like natural disasters or hospital visits.

### Reputation Attacks

Deepfake media portraying executives or company representatives in damaging scenarios (e.g., discriminatory statements or misconduct) can spread rapidly on social media. Even if disproven, these events can erode trust, reduce policy renewals, and trigger regulatory scrutiny.

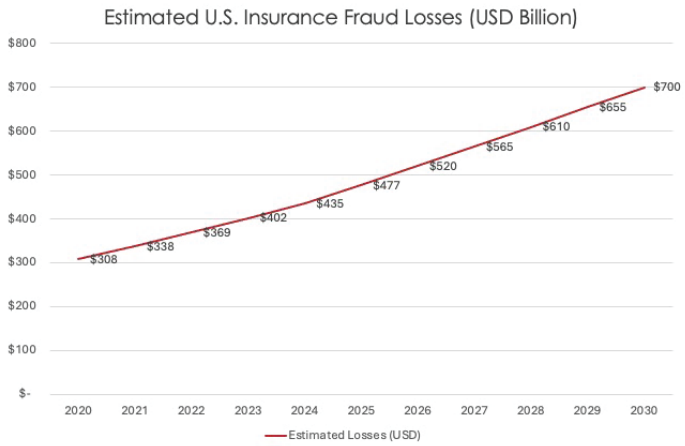
### Executive Communications & Internal Social Engineering

As insurers adopt digital tools like video memos and live streams, these internal channels are becoming targets for deepfake attacks. Cybercriminals impersonate executives to issue fake directives—such as financial transfers or password resets—exploiting the trust and urgency tied to senior leadership. These "video whaling" attacks are especially effective in high-pressure situations where employees may act without verification.

www.hitechadvisors.com hello@hitechadvisors.com (425) 284-3315

# Notable Incidents and Industry Signals

Insurance fraud is accelerating at a concerning pace. According to the Coalition Against Insurance Fraud, annual losses across U.S. insurance lines are estimated to exceed $308 billion today. If current trends continue—driven by both traditional schemes and emerging tactics like deepfakes and synthetic identity fraud—total losses could approach $700 billion by 2030, based on internal projections. This sharp upward trajectory reflects a growing threat landscape in which AI-generated media is already being used to manipulate claims, impersonate agents, and undermine onboarding systems. The following examples highlight how these technologies are actively reshaping the industry's exposure to fraud and deception.




**Voice-Cloned CEO Scam (2020, UAE Bank)**

In a high-profile 2020 case, fraudsters used AI-generated voice cloning to impersonate a corporate executive and deceive a bank into transferring $35 million. The attackers mimicked the speech and accent of the company's director and coordinated with a network of accomplices to submit fake legal documents and emails supporting the transaction. The UAE-based firm did not detect the fraud until after the funds were dispersed across multiple accounts. Authorities later confirmed that the voice used in the phone call had been synthetically generated using advanced AI tools—one of the earliest confirmed deepfake-enabled wire fraud cases in the financial sector.[1]

**Energy Firm CEO Impersonation (2019, UK)**

In 2019, a UK-based energy company's executive was targeted by a sophisticated voice-deepfake attack that led to the fraudulent transfer of €220,000. The attackers used AI-generated audio to replicate the voice of the firm's parent company CEO, instructing a subordinate to complete the wire transfer urgently. The voice matched the CEO's accent and cadence closely enough to bypass suspicion. The attack was successful because it leveraged urgency, familiarity, and authority—making it one of the first commercially reported uses of AI voice cloning in business fraud. While no insurance firm was targeted, the case has since become a cautionary benchmark for impersonation risks across high-trust industries.[2]

**Zelenskyy Deepfake Disinformation Attack (2022)**

In 2022, a deepfake video of Ukrainian President Volodymyr Zelenskyy calling for his country's surrender circulated online after hackers compromised a Ukrainian news outlet. The video featured realistic facial animation and voice cloning, and briefly aired on both social media and the news channel's livestream. While quickly debunked, the incident demonstrated how deepfakes can be used to manipulate public perception, disrupt trust in leadership, and spread disinformation at scale. For insurers, such events highlight the potential for synthetic media to cause reputational damage and erode consumer confidence—even without direct financial fraud.[3]

www.hitechadvisors.com

hello@hitechadvisors.com

608 State Street South
Kirkland, WA 98033
(425) 284-3315

[1] Bloomberg. "Deepfake Used to Scam a Bank Out of $35 Million."
[2] Wall Street Journal. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case."
[3] NPR. "A Deepfake of Ukraine's President Saying 'Surrender' Was Fake, but Shows New Threat."

HITECH ADVISORS

As deepfake-enabled fraud becomes more advanced, insurers must move beyond traditional defenses. Synthetic media is now used to impersonate policyholders, forge claims, and bypass onboarding processes—posing serious risks to trust, compliance, and operations.

To counter these threats, insurers need a layered defense strategy that combines advanced detection technologies, human expertise, and resilient workflows. The strategies below highlight how insurance organizations can identify and mitigate deepfake risks before they cause harm.

## Advanced Technologies

Modern deepfake detection tools use AI to analyze video and audio for subtle signs of manipulation—like irregular facial movements, pitch shifts, or lighting anomalies. These systems can flag suspicious content in real time or during claims review and onboarding, serving as an early line of defense.

Biometric liveness checks confirm the presence of a real person by analyzing micro-movements, blinking, and speech patterns—critical for remote claims or onboarding where in-person verification isn't possible. Document forensics tools detect synthetic IDs by scanning for metadata issues, font mismatches, and tampering. Paired with identity intelligence, they help flag repeat offenders or known synthetic personas.

Cross-channel correlation enhances fraud detection by linking behavioral, device, and transaction data. If patterns deviate from a user's history, the system can trigger further checks, providing context-aware validation beyond static inputs.

## Human Vigilance

While AI tools are essential, they are most effective when paired with trained human analysts. Claims examiners, call center agents, and underwriters should be educated to recognize deepfake indicators such as strange audio delays, visual mismatches, or inconsistencies in applicant behavior. Continuous learning programs and playbooks can help them adapt to new attack techniques.

Red team simulations using synthetic content should be conducted to test organizational resilience. These exercises can mimic deepfake impersonation of agents, forged video evidence submissions, or synthetic onboarding, helping insurers identify vulnerabilities in real-world scenarios and refine their response protocols.

## Hardened Workflows

Insurers should implement second-factor verification for high-risk transactions, such as large claim payouts or updates to bank details. This could involve a callback from a separate department, in-app push verification, or a biometric re-authentication step to ensure legitimacy.

Integrating provenance tracking and timestamping capabilities for user-submitted media provides another layer of defense. These tools validate when and where a video or image was captured, helping to distinguish between authentic submissions and synthetic forgeries. When embedded into claims intake platforms, they provide an audit trail and allow faster dispute resolution.

www.hitechadvisors.com hello@hitechadvisors.com (425) 284-3315

# Governance, Risk, and Regulatory Considerations

Insurers must ensure their efforts to combat deepfake threats are not only technically robust but also aligned with broader Governance, Risk, and Compliance (GRC) priorities. As regulatory scrutiny grows and synthetic media becomes a recognized risk, GRC leaders must embed deepfake resilience into their enterprise frameworks.

## NAIC Guidance Compliance

The National Association of Insurance Commissioners (NAIC) has introduced AI principles focused on fairness, accountability, and transparency. These principles apply directly to insurers using or defending against AI-driven technologies like deepfakes. Carriers are expected to demonstrate transparency in AI model deployment and ensure that systems do not unintentionally harm consumers. As deepfake detection becomes part of automated decision-making in claims or onboarding, compliance with NAIC expectations around explainability and bias mitigation becomes crucial.

## ERM Integration

Enterprise Risk Management (ERM) frameworks should now explicitly include deepfakes as a recognized operational and reputational risk. This requires insurers to assess deepfake risk exposure across functions—underwriting, claims, IT, customer service—and define mitigation strategies within their risk registers. Boards and executive teams should be briefed on synthetic media trends and the institution's preparedness. Incorporating deepfake scenarios into annual risk assessments, incident response playbooks, and GRC dashboards ensures that the organization is not caught off guard by this evolving threat landscape.

## State Regulator Scrutiny

Several state insurance commissioners are now proactively assessing how carriers are protecting against emerging digital fraud—including synthetic media threats. Insurers may be required to report on cybersecurity posture, detection capabilities, and vendor controls during audits or rate filings. States like California and New York have begun integrating digital fraud prevention into broader solvency and consumer protection reviews, signaling that synthetic fraud is now a board-level compliance issue.

## FTC and SEC Oversight

The Federal Trade Commission (FTC) has issued warnings about the use of synthetic media in deceptive practices, and insurers could face penalties if deepfakes are used in policyholder communications or advertising without proper safeguards. Additionally, for publicly traded insurers, the Securities and Exchange Commission (SEC) expects timely disclosure of material cybersecurity incidents—including those involving synthetic fraud or reputational harm. As synthetic threats can compromise customer trust and brand equity, insurers must treat them as potential material events.

As synthetic media threats grow, insurers must align their defense strategies with evolving regulatory expectations. Deepfakes now fall under the purview of bodies like the NAIC, FTC, SEC, and state regulators—each emphasizing transparency, consumer protection, and timely incident reporting. Insurers are urged to integrate deepfake risk into Enterprise Risk Management (ERM) frameworks, adapt compliance programs to meet AI governance standards, and prepare executive teams for heightened scrutiny. Staying ahead means not just detecting deepfakes—but proving you did so responsibly.

www.hitechadvisors.com hello@hitechadvisors.com (425) 284-3315

# Strategic Response Plan by Hitech Advisors

As synthetic media threats accelerate, insurance leaders must move from awareness to action. Defending against deepfakes requires more than deploying new technology—it demands a strategic, enterprise-wide response that bridges operations, cybersecurity, compliance, and customer trust. The following action plan outlines five key initiatives insurers can implement to proactively identify vulnerabilities, strengthen digital defenses, train their workforce, and embed synthetic media resilience into core governance practices.

## 1 Conduct a Synthetic Risk Assessment

The first step in building resilience against deepfakes is understanding where vulnerabilities exist. Insurers should evaluate exposure across key business functions, including underwriting, claims, customer service, and fraud detection. This involves mapping where audio, video, or document-based inputs enter workflows and assessing how these assets are currently authenticated. A formal risk assessment should also account for third-party exposure, such as digital communications platforms or vendor-provided onboarding tools. The goal is to identify choke points where synthetic media could be injected and evaluate existing controls.

## 2 Invest in Detection & Verification Technologies

To stay ahead of synthetic threats, insurers must pilot or integrate deepfake detection solutions into their digital ecosystems. This includes deploying AI-driven media analysis tools that can scan submitted videos or audio for tampering signs, as well as implementing biometric verification systems that check for liveness during identity verification. Cross-channel authentication—linking biometric, behavioral, and device data—adds another layer of defense and can be used to flag anomalous activities during claims or account updates. Investments should be prioritized in high-risk areas like remote claims submission and agent/policyholder communications.

## 3 Train for Recognition and Response

Technology alone isn't enough—your people need to be prepared. Deepfake awareness should be added to fraud prevention training programs, claims certification curricula, and standard operating procedures for customer-facing teams. Staff should be trained to identify signs of synthetic manipulation, such as unnatural speech patterns, odd lighting artifacts in video, or discrepancies in caller behavior. These frontline employees play a critical role in detecting what AI might miss. Training should be role-specific and refreshed frequently as the threat landscape evolves.

## 4 Simulate Synthetic Threat Scenarios

Simulations and tabletop exercises provide a safe environment to test preparedness. These scenarios might include a deepfake impersonation of an executive requesting a policy payout, a synthetic customer onboarding through video KYC, or fake media submitted as part of a claim. Running these drills helps stress-test workflows, expose procedural weaknesses, and sharpen cross-functional coordination. Exercises should include IT, legal, compliance, claims, fraud, and communications teams to ensure comprehensive response capability.

## 5 Update Governance Policies

Insurers must codify their synthetic threat posture within corporate governance frameworks. This includes updating cybersecurity and fraud policies to include detection and response procedures for deepfakes, assigning ownership for synthetic risk monitoring, and ensuring that board-level risk registers reflect this new class of threats. Policies should also guide the use of synthetic media internally—for example, barring unauthorized use of AI-generated content in marketing or agent communication without clear disclosure. Clear governance provides the foundation for consistent enforcement and accountability.

# HITECH ADVISORS

READY TO BUILD YOUR

DEEPFAKE DEFENSE ROADMAP?

Our experts are here to help.

## About Hitech Advisors

Hitech Advisors helps insurance carriers and service providers anticipate and respond to the next generation of digital threats. Our cybersecurity, fraud detection, and governance teams bring deep expertise in AI-driven risk. From simulating synthetic fraud to implementing verification systems and supporting NAIC readiness, we guide insurers through complex transformation with clarity and trust.


**WEBSITE**

www.hitechadvisors.com

**EMAIL**

hello@hitechadvisors.com

**PHONE**

(425) 284-3315