THALES

CYBERSECURITY

Deepfake Fraud

Protection Strategies for Airlines

In the age of Generative Artificial Intelligence (Gen AI), airlines face increasing threats from sophisticated fraud techniques, including deepfakes, through Identity Spoofing. This becomes especially concerning for carriers anaging millions of passenger accounts, loyalty programs, and corporate travel platforms. Several data breaches over the years have left almost everyone vulnerable. Fraudsters can pick up nuggets of compromised "real" data to create Synthetic Identities. For finesse, AI-generated synthetic media can convincingly mimic real individuals, posing significant risks during digital onboarding and account management processes. To combat these threats, airlines must adopt a multi-layered approach beyond just Identity Proofing with Multi-Factor Authentication (MFA), Liveness Detection, Behavioral Biometrics, and robust Risk Management strategies.

Multi-Factor Authentication (MFA)

MFA is a critical first line of defense against deepfakes. By requiring multiple forms of verification, such as something the user knows (e.g., a password), something the user has (a smartphone), and something the user is (biometric data), MFA significantly reduces the likelihood of unauthorized access. For instance, even if a deepfake video is used to bypass facial recognition, the fraudster would still need to provide additional authentication factors, making it much harder to succeed. So, adopt MFA - go Passwordless!

Liveness Detection

Liveness detection technology is designed to distinguish between real, live human beings and static images or videos. This technology can detect subtle movements, such as blinking or changes in facial expression, that are difficult for deepfakes to replicate convincingly. By integrating liveness detection into the onboarding process, airlines can ensure that the person on the other end of the camera is indeed a live individual and not a sophisticated deepfake.

Behavioral Biometrics

Behavioral biometrics analyze patterns in user behavior, such as typing speed, mouse movements, and navigation habits. These patterns are unique to each individual and difficult for fraudsters to mimic. By monitoring these behaviors, airlines can identify anomalies that may indicate fraudulent activity. For example, if a user's typing pattern suddenly changes, it could be a sign that someone else is attempting to impersonate them.

Risk Management

A comprehensive **risk management** strategy is essential for preventing fraud. This involves continuously monitoring and analyzing data to identify potential threats and vulnerabilities. Airlines should implement real-time fraud detection systems that use machine learning algorithms to detect unusual patterns and flag suspicious activities. Additionally, regular audits and updates to security protocols can help ensure that the airline remains resilient against evolving threats.

How can Thales Help Address these Challenges?

Thales offers a range of solutions that can significantly enhance security measures against deepfakes in digital customer flows for airlines. Here's how Thales can help with each of the key strategies:

Multi-Factor Authentication (MFA)

Thales provides robust MFA solutions that combine various authentication methods to ensure secure access. Their solutions include:

- **Thales OneWelcome Identity Platform:** A cloud-based Customer Identity and Access Management (CIAM) solution that supports a wide range of authentication methods, including OTP, PKI, and FIDO protocols.
- **Thales Authenticators:** These address multiple use cases and threat vectors, offering both hardware and virtual smart cards, tokens, and mobile authenticators.

Liveness Detection

Thales has advanced liveness detection technologies to prevent spoofing attacks:

- **Face and Fingerprint Liveness Detection:** Thales uses AI and deep learning algorithms to detect whether a biometric sample is from a live person or a spoof artifact. This technology analyzes subtle movements and other indicators to ensure the authenticity of the biometric data.

Behavioral Biometrics

Thales integrates behavioral biometrics into its security solutions to enhance fraud detection:

- **Behavioral Analysis:** By monitoring user behavior patterns such as typing speed, mouse movements, and navigation habits, Thales' solutions can identify anomalies that may indicate fraudulent activity.

Risk Management

Thales offers comprehensive risk management tools to continuously monitor and mitigate potential threats:

- **Advanced Fraud & Risk Management:** Thales employs machine learning algorithms to detect unusual patterns and flag suspicious activities in real-time, helping airlines stay ahead of evolving fraud techniques.
- **Compliance and Security Protocols:** Thales ensures that their solutions comply with regulatory requirements and are regularly updated to address new security challenges.

A Multi-Layered Approach

By leveraging Thales' advanced technologies in Identity Proofing, MFA, liveness detection, behavioral biometrics and robust risk management tools provides a formidable defense against deepfakes. This multi-layered approach not only protects sensitive information but also fosters trust and confidence among passengers and business partners.
As fraud techniques continue to evolve, staying ahead of the curve with advanced security measures is not just an option but a necessity.