

AirFi and IdeaNova discuss industry security practices for digital data

This is a special feature from the [April 2025 AIX issue](#) of PAX Tech Magazine, on [page 10](#).



Secure onboard payment

As the push for a more digitized onboard experience gathers pace, the associated usage by passengers of personal electronic devices (PEDs) introduces new layers of vulnerability and security threats into the cabin. With greater convenience comes greater risk to personal data.

Every good security implementation uses several layers, and fortunately, help is at hand for airlines to call upon to deploy such measures. One relatively simple layer used [IdeaNova](#) is based upon the principle of “need to know.”

As CEO Juraj Siska explains, passenger data is only collected and accessible if needed. The second, and more sophisticated, is to leverage technology available either on a PED or an IFE server.

“Anything from hardware encryption via TPM and SGX to software encryption is used by our products,” he says.

[AirFi](#) CEO Job Heimerikx says the company uses full Payment Card Industry (PCI) certification for payment security, applying the same encryption standards to passenger data, which tends to remain on personal devices rather than being centrally stored, reducing risk. Unauthorized access is further prevented by AirFi’s system architecture, which requires physical presence on an aircraft to attempt a

breach. Even in the event of an attempted attack, extensive security measures are in place, states Heimerikx, who adds that AirFi tracks intrusion attempts, allowing for the identification and tracing of bad actors.

Ensuring safeguards



Juraj Siska, CEO, IdeaNova

“Proper defense starts at design,” emphasizes Siska, who says IdeaNova leverages OWASP (Open Worldwide Application Security Project) best practices. “We bake security right into the design and architecture of our products. We also realize that secure systems cannot be built by untrained professionals, therefore we spend time on continuous training. Each developer is required to complete several modules of Security Shephard training per month.”

Each product is subject to vulnerability scanning before its release, while AirFi says all its hardware and services undergo rigorous annual penetration testing by ethical hackers.

Additionally, IdeaNova monitors trends and counsels its customers about common vulnerabilities that might need to be addressed either by applying software patches or a complete system update.

Defeating deception



Job Heimerikx, CEO, AirFi

AirFi's connectivity solution is already leveraged by key industry partners to eliminate fraud and boost onboard retail operations through real-time payment validation. The company collaborates with leading payment industry experts like [Perseuss](#), [Mastercard](#), and [Worldpay](#) to create an integrated fraud prevention ecosystem. Together, they are working to bring the same fraud management protocols used in e-commerce on the ground to inflight systems.

"We prioritize security by operating primarily offline, minimizing exposure to online threats," says Heimerikx. He explains that payment information is securely transmitted via the company's LEO inflight connectivity system to the ground, where it is verified before being relayed back to the crew. "This process ensures that transactions are completed successfully and reduces fraud to nearly zero percent," he claims.

Siska believes that connectivity provides yet another vector of attack and therefore should be considered when building new systems and enabling connectivity on the aircraft. "We monitor the cyber security landscape and notify our customers as new threats emerge and coordinate possible mitigation," he says.

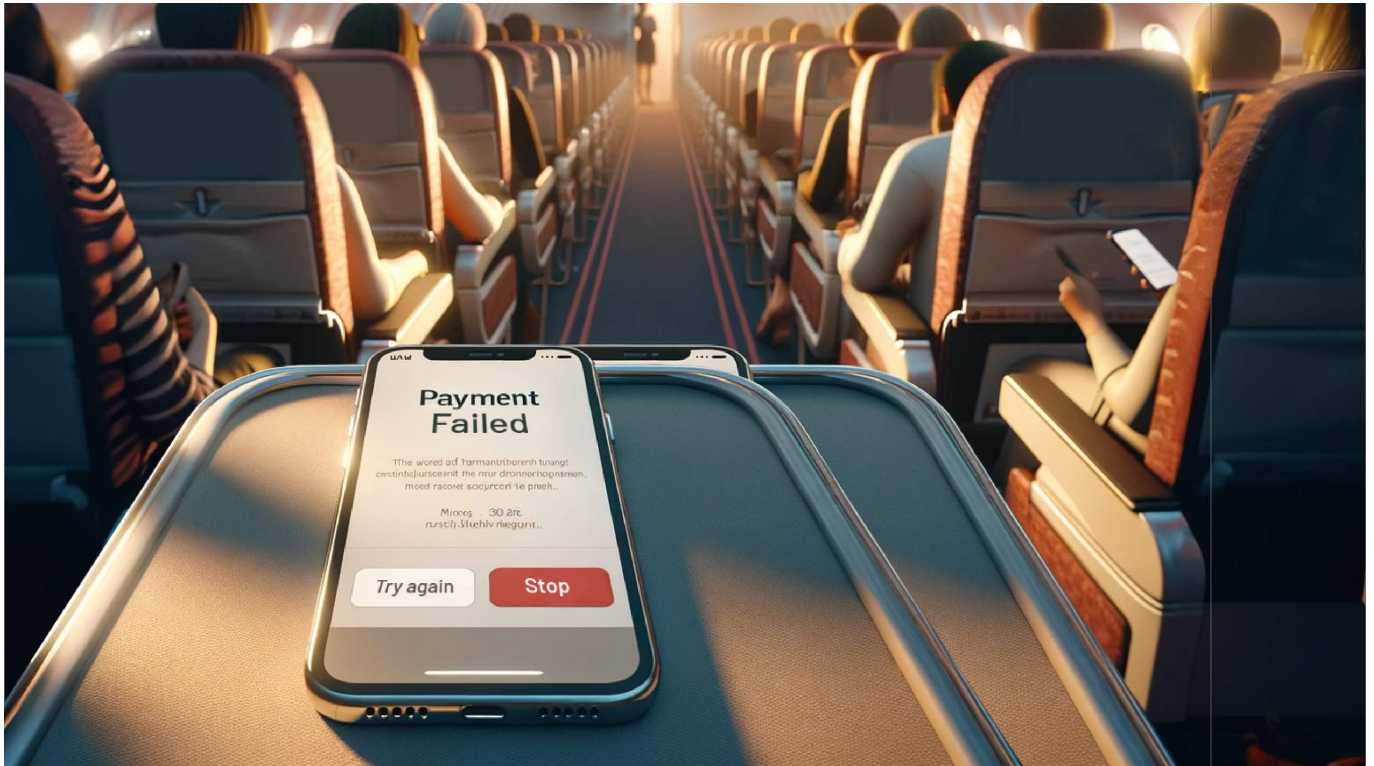
For its part, AirFi invests heavily in cybersecurity to meet industry standards and compliance. As Heimerikx points out, however, a key differentiator for the company is that its system operates independently from the aircraft, requiring no direct connection, which eliminates risks related to flight safety and aviation cybersecurity regulations.

“As a result, AirFi has minimal need to collaborate with regulatory bodies on broader aviation cybersecurity concerns,” says Heimerikx.

As the aviation industry moves toward greater connectivity, he says AirFi remains focused on securing its platforms without impacting flight safety or requiring direct integration with the aircraft.

“From our perspective, collaboration with airlines is a lot more relevant, particularly regarding the security of back-office systems and passenger data collection. In this area, AirFi adheres to industry-standard cybersecurity measures, undergoes periodic audits, and follows best practices from the e-commerce and IT industries to ensure compliance and security,” Heimerikx adds.

A time for AI?



AirFi collaborates with leading payment industry experts for secure inflight payment

Could AI play a role in best practice? The jury is still out on this question. AI and machine learning are not yet primary tools for cybersecurity at AirFi, as the technology is still evolving in this field, Heimerikx tells *PAX Tech*.

The company leverages AI to enhance the passenger experience rather than for security purposes, as its role in real-time cyber threat mitigation remains uncertain. AirFi’s system architecture, including that of its offline operations and AirFi LEO connectivity, is designed in a way that does not require AI-driven cybersecurity solutions.

“AI, just like any new technology, can be used to enhance security posture by analyzing suspicious patterns or can be misused when in the hands of malicious users. It will take a human to dissect the information, put it to good use and identify its use for enhancing our flying experience,” says Siska.