



vProtect

Reduce in-flight fraud with our secure, modular,
PCI DSS-compliant fraud prevention solution



Retail inMotion

An industry plagued by onboard fraud

Airlines that have not adopted technology for online in-flight payments create opportunities for perpetrators to exploit the POS system's inability to instantly authorise transactions.



Across the evaluation period, (June 2023 to July 2024)*, almost ~£20M of in-flight purchases using Mastercard cards issued in the UK were declined post release of the merchandise.

Whilst reported fraud is less than 1bp, these declines constitute a significant direct loss to airlines representing ~4% of total in-flight sales.

Considering that these metrics only contain UK Mastercard issued cards, the extent of losses will be more severe across the entire payment ecosystem.

What if a fraud prevention platform could facilitate blocking cards, to reduce not only future onboard use of the card, but wider online payment abuse, easier recovery of revenue and industry collaboration to help in the global fight against sophisticated fraudsters?

Welcome to vProtect

At Retail inMotion, we are global retail experts, providing onboard retail programs and integrated technology solutions to international airlines for over 20 years, processing over a billion dollars in in-flight payments annually.

vProtect is our new modular, PCI DSS-compliant, fraud prevention solution, integrated with our proprietary Vector ecosystem, specifically developed to tackle airline fraud.

It uses secure precise data, intelligent feedback loops and industry collaboration to stop fraud before it happens – without compromising legitimate sales.

*(Source: Mastercard Airline in-flight acceptance abuse Research Report)



Retail inMotion

Introducing vProtect Features



Each feature can be enabled independently or in parallel

FEATURE OVERVIEW	WHAT DOES IT MEAN FOR YOU?
Hard decline auto protect Secure protection from use of known fraudulent payment methods.	This prevents further use onboard of a fraudulent card and reduces the airline's rate of fraud.
Soft decline auto protect Secure blocking of 'soft' declined payment attempts with the ability to remove the block if the funds are recovered after retrying the authorisation.	This prevents further use onboard of a potentially fraudulent card and reduces the airline's rate of fraud while resubmissions are on-going.
Board pass/card scans Allows the scanning of a passenger's boarding pass/card when making in-flight purchases for transactions over a pre-defined limit or product range.	This deters would-be fraudsters and allows the airline to match the purchase to the customer, enabling easier recovery of funds for declined payments if and when required.
vProtect upload interface Secure, self-service method for issuers, schemes and airlines to add known fraudulent full PANs directly to vProtect.	This allows airlines and merchants to stop further fraud from known fraudulent cards.
Revenue recovery payment links Enables the sending of a payment link post-flight to a passenger whose transaction has been declined, so that they can pay easily and be removed from vProtect.	This allows for smoother recovery of revenue and reduces fraud for the airline and merchant.
vProtect Risk Management Platform API Integration with existing online risk management platforms to enable sharing of declined data with the existing airline partner.	This helps the airline identify the customer to recover funds and prevent suspected fraudsters from making future online ticket purchases. It narrows the gap between online and in-flight fraud, ensuring fraudsters are tracked and monitored at all times.
vProtect Open API Secure API available to airlines who do not currently partner with Retail inMotion.	This enables other airlines to consume vProtect decline data and prevent fraud.





Why airlines choose vProtect?

✓ **Fraud Protection**

vProtect protects airlines against future fraudulent activity both at a hard and soft decline level - helping save money and reduce in-flight and online payment fraud.

✓ **Increased Acceptance**

vProtect uses precision protection by targeting the full PAN, removing the risk of false declines and making the sales process smoother, faster and easier for crew.

✓ **Revenue Recovery Tools**

vProtect turns failed payments into recovered revenue.

✓ **Scheme Compliant**

vProtect ensures merchants and acquirers are compliant with scheme rules to honour all cards.

✓ **PCI DSS Compliant**

vProtect adheres to all Retail inMotion and PCI DSS security policies and standards to ensure full PCI DSS-compliance.

✓ **Metrics and KPIs**

vProtect has its own reporting portal where customers can measure performance in near real-time.

✓ **Robust Industry Partnerships**

Retail inMotion has identified key partners to narrow the gap between online and deferred authentication applications and, due to these partners' existing relationships with multiple airlines, integration is simpler, faster and more secure.

✓ **Dedicated Account Manager**

Each airline has a dedicated account manager to provide comprehensive support for the product.

✓ **vProtect UI**

vProtect has its own User Interface where each customer can securely login and manage elements of their account blocklist.

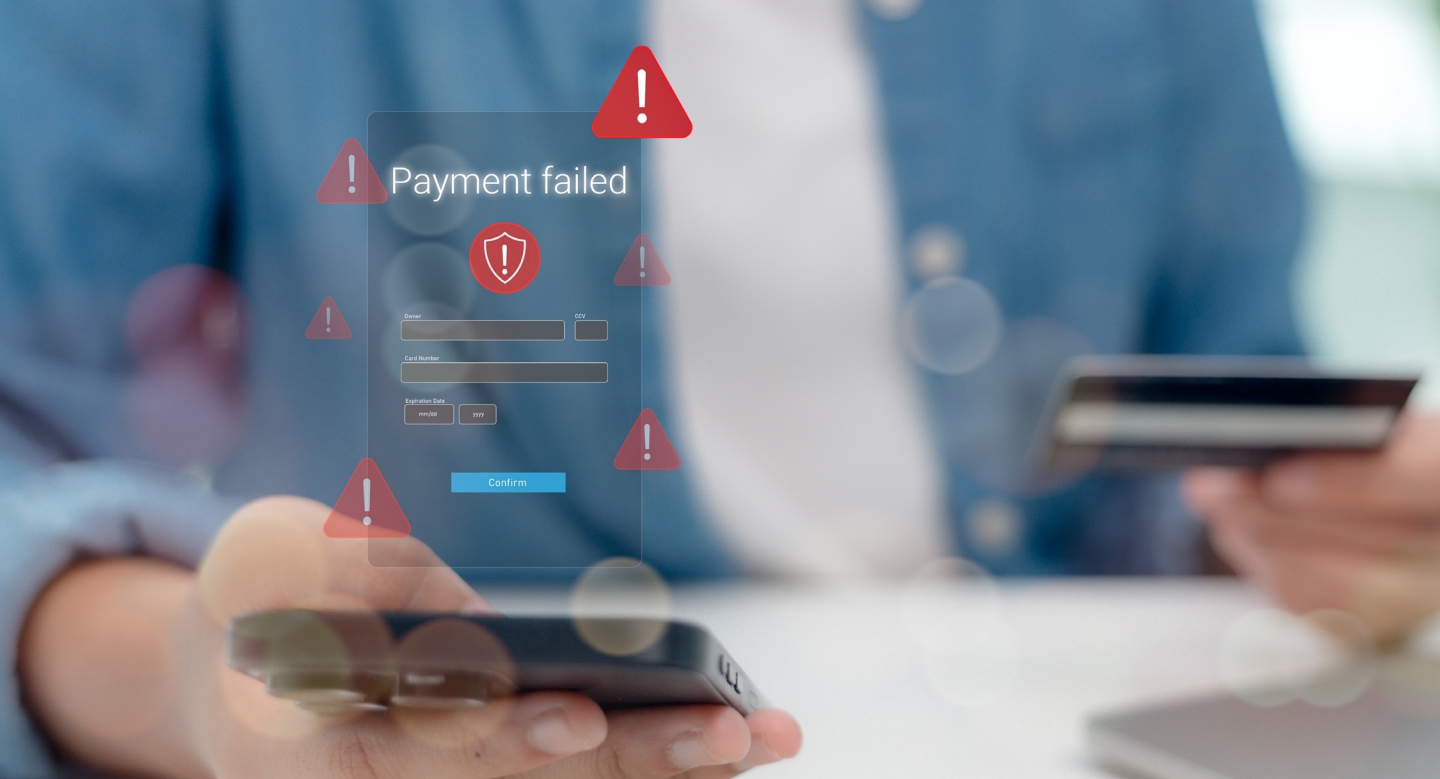
✓ **Issuer & Scheme Participation**

Issuers and schemes have user access to permit them to add entries to vProtect.

✓ **24/7 Support**

Retail inMotion provides 24/7 support via our dedicated service desk.





Product Features in more detail

Hard decline auto protect

When a bank declines a request for authorisation, it responds with a code that describes the reason for the decline. These reasons can be split into various categories and the categories grouped by 'hard decline' (the bank will never approve), for example, '04 - Retain Card', and 'soft decline' (the bank may approve but cannot approve right now), for example, '51 - Insufficient Funds'.

When Retail inMotion receives a 'hard decline' in response to a request for authorisation, it adds the full PAN (Primary Account Number) to a common blocklist. The PANs are hashed, encrypted and copied to the secure element on the Point of Sale (POS) terminal, known as vPayConnect, once the POS has been successfully synced. Any further attempts to pay for goods onboard with such cards are blocked.

Soft decline auto protect

A 'soft decline' is a grouping of authorisation response codes that indicate a bank may approve the request for authorisation but cannot right now. The most common cause a bank declines for this reason is where the card holder is attempting to pay but does not have sufficient funds behind the card.

In our experience, despite the schemes having mandated to do so, issuers have been seen to not respond with the appropriate response code from time to time. For example, where an issuer responds with a '05 - Do Not Honour' response code but in fact the account had no funds, and response '51 - Insufficient Funds' should have been received. We also see banks may respond with a soft decline response when a hard decline response would have been more appropriate. For this reason, Retail inMotion is introducing soft decline protection to prevent fraudsters from multi-trip, repetitive fraud abuses onboard with the same card.

When a soft decline is received from the issuer, vProtect will add this full hashed and encrypted PAN to the customer specific vProtect list. Retail inMotion's Payment Gateway retries soft declines in accordance with scheme resubmission rules and, should the funds be recovered via such retries, the payment gateway will notify vProtect to remove the card. If funds have still not been recovered after the allotted retry cycle timeframe, the full PAN will remain on the soft decline element of vProtect to allow for removal in the future should funds be received via other avenues.



Boarding Card Scanning – PNR Recording

When a passenger attempts to purchase onboard items exceeding a pre-agreed limit, they will be asked to produce their boarding card for scanning. This is no different to what happens on the ground in the airport today.

The purpose of this action is to:

- match the passenger details scanned to the passenger manifest so that if the payment is subsequently declined upon landing, the airline can contact the passenger to recover funds; and
- deter a would-be fraudster from attempting to commit fraud.

vProtect Upload Interface

Retail inMotion is regularly contacted by Issuers looking for certain cards to be restricted from being used for in-flight purchases. This is currently a manual process, however vProtect exposes a secure, self-service method for issuers, schemes and airlines to add known fraudulent cards to vProtect themselves. Issuer and scheme entries will be added to the common list whereas airline entries will be added to the customer specific list.

vProtect Risk Management Platform Integration

vProtect integrates with existing risk management platforms, currently used by most airlines, to prevent fraud in the airline online ticket sales domain. It is primarily a rules-based engine that uses multiple, diverse datasets to score the payment attempt and influence an accept/decline decision when payment is being attempted.

Using scanned boarding cards and a Decision Validation System (DVS) API, vProtect passes declined data to the airline to:

- identify the passenger and help recover funds; and
- prevent suspected fraudsters from making further ticket purchases.

Revenue Recovery

Today, when a passenger is made aware that their onboard purchase was declined by their bank, there is no mechanism in place to allow them to attempt to repay. With vProtect, payment links are created that open a user interface and permit the passenger to pay online. As Retail inMotion does not currently collect passenger details when they pay, it relies on the airline to try and identify the passenger. Using scanned boarding cards assists in identifying the passenger and thus forwarding the payment links to the correct passenger for payment.

Open API

This will allow airlines that don't work directly with Retail inMotion to securely consume vProtect data and prevent onboard fraud.





Deprecation of existing blocklist service

We plan to phase out our existing blocklist solution in favour of vProtect from **31 December 2025**. This is required to demonstrate to the card schemes that all merchants are compliant with scheme rules to honour all cards.

How do I enable vProtect?



vProtect can be enabled in 4 simple steps



Ensure all Pin Entry Devices (PEDs) are injected with the latest vProtect security and encryption keys.



Ensure your current version of vPOS in the field is vProtect compatible.



Update to the 'GetvProtect' API in your Vector back-office instance.



Complete the synchronisation for all POS terminals to activate protection.



Retail inMotion



FAQs

How is the vProtect blocklist populated?

The list is populated via the hard and soft decline response codes received from acquirers and associated issuer banks. This is an automated process and Retail inMotion does not enter card details to this list. Via the new upload interface, schemes, issuers and airlines will be able to manually add cards also.

What are the differences between the application of these hard and soft response code elements of this vProtect list?

Hard decline responses received by Retail inMotion form the common vProtect list – this is in turn applied to all customers using vProtect and managed by Retail inMotion alone. The soft decline element is customer specific due to the nature of how these cards can be added and removed from the list.

How does vProtect keep card numbers safe?

Restricted cards are hashed and encrypted to secure the full PAN (Primary Account Number).

How does vProtect differ from how Retail inMotion protects against fraud today?

Precision protection by using the full PAN prevents false declines, revenue recovery tools recoup potentially lost funds, and blocklist functionality assures a market-leading fraud mitigation solution.

How are DPANs (Device Primary Account Numbers) handled by vProtect?

DPANs are treated in the same, secure way as FPANs (Funding Primary Account Numbers) – where an FPAN is the actual full card number printed on a card and the DPAN is the tokenised version of this FPAN, generated when you add a card to a digital wallet (e.g. Google Pay, Apple Pay).

How will I be able to analyse the active vProtect blocklist in place?

Existing Vector reports will remain in place for now to allow a full review of what is contained in vProtect. These cards will be stored in the backend as the full PAN but visible in Vector as First 6, Last 4 due to PCI DSS requirements and security standards.

Let's Talk

Ready to protect your onboard revenue with the most advanced fraud prevention platform in the skies?

Contact your Retail inMotion Account Manager.

Terms and Conditions apply



Retail inMotion

Dublin, Ireland

Building 11,
Cherrywood Business Park,
D18 DH50,
Dublin 18,
Ireland.

Frankfurt, Germany

Speicherstraße 1,
60327, Frankfurt am Main,
Germany.

E: info@retailinmotion.com

