



ACCOUNT SECURITY



TURKISH AIRLINES

brief introduction

Preventing Large-Scale ATO Attacks, Building Advanced FFP Security, and Charting Our AI Roadmap.

Orhan ÖZEN

Account Security Analyst



What We Will Cover Today ?

The Same Attack, Two Different Years (2025 vs 2026)

We will walk through the same ATO attack in two different years — showing how both the attack and our response evolved.

Other Real Cases

A few additional fraud scenarios we managed to detect and stop.

Our AI Roadmap

Where we are heading next and how AI will support proactive security.

Recap of Paris

A quick look at what we shared last year and the key challenges we identified at that time.

Comparison & Key Learnings

Two different outcomes — and what made the real difference.

Building Advanced Account Security

How we are moving towards more dynamic, intelligence-driven, multi-layered security capabilities.

A Quick Trip Back to Paris - 2025

Time To Change The Game; Pushing Limits & Raising the Bar in FFP Security Fundamentals, Challenges & Solutions

From a Minor Team to a Strategic Asset

With strong leadership
support, a dedicated Account
& Transaction Security
department was established.

Escalating the Issue: A Turning Point

As the account security team,
we raised concerns directly to
leadership.

Building the Roadmap for Advanced FFP Security

We shared a clear roadmap to
develop a more advanced FFP
security solution. A step-by-step plan
to move towards stronger and more
scalable protection.

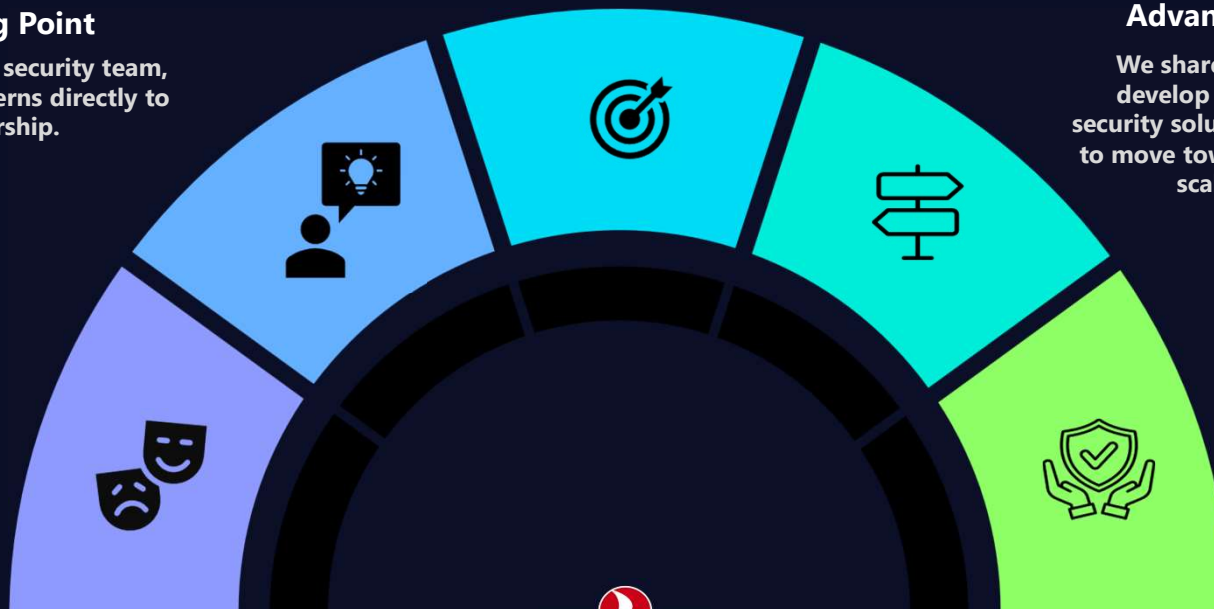
Delivering on Our Promise

Last year in Paris, we presented our
roadmap and promised to return this
year with our progress.

We kept our promise.

The gap: Payment vs FFP Security

We highlighted the gap —
and this gap still exists today.



WHY THIS CASE ?



Step By Step

What Happened?



Step 1

Publication of fake campaign ads across multiple social media platforms



Step 2

Many members trusted the ads and clicked → redirected to a fake login page



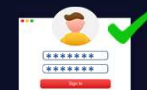
Step 3

System simultaneously opened the real Miles&Smiles login page to start the actual login process



Step 4

Members entered their Account ID and PIN, then submitted the OTP code



Step 5

Automated system used the stolen credentials to successfully log into the real accounts



Step 9

Fraudsters logged into the Shop&Miles store and converted miles into gift cards



Step 8

Some members noticed they received a "phone number change" SMS instead of a registration confirmation



Step 7

System used the submitted OTP to change the registered GSM number



Step 6

Members were asked to register to the campaign using OTP authentication



Step By Step

How We Handled the Attack (2026) ?

Detection

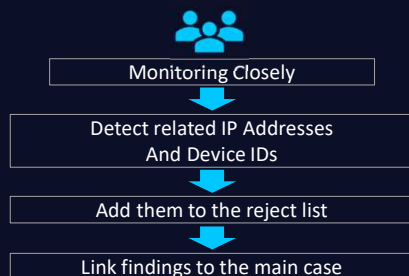


We detected an abnormal spike in redemptions from the same digital points (IPs) and simultaneously received a wave of customer complaints.

Setting First Rule & Team Response



Even though some system components were still under development, we quickly deployed our first rule: Reject redemption if the IP address or Device ID matches the blacklist.



Impact of the rule



The rule initially worked very well. Fraudsters were caught off guard — there was no 24-hour delay and only a limited number of accounts were compromised at first.

However, they noticed that our monitoring and rule enforcement were significantly weaker during weekends. Then they adapted and began concentrating their attacks especially on weekend hours.

Velocity Rules



To close this gap permanently and achieve true 24/7 protection, we accelerated the development and activated our Velocity Rules engine — a real game changer.

This new capability enables dynamic, real-time behavioral rules. Example: If a single Device or IP interacts with more than X Frequent Flyer Profiles within a short time window → automatic rejection.

Full 24/7 protection No manual effort required for this attack pattern Rules deployed only two weeks ago.

The newly developed Case and Link Management capability played a critical role — it allowed us to efficiently link related IPs, Device IDs, and campaigns to the main attack. This improved our visibility, coordination, and ability.



Comparison

What is the difference between both attacks regarding impacts?

2025



No Rule in Place



Large number of accounts compromised



Many members negativley affected
due to 24-hour delay action



24-hour delay caused significant
damage to the bussines

VS

2026



Dynamic Rules Activated



Less number of accounts compromised



No need for 24 our delay



No damage to bussines



Other real cases

That We Successfully Stopped with Rules

01



Credential Stuffing Attack

A large-scale credential stuffing campaign was detected targeting thousands of accounts from the same source. We immediately applied a targeted **OTP rule** and stopped the attack.

02



Proactive ATO Risk

We received intelligence about a potential data breach. We quickly defined a high-risk member segment and deployed a preventive OTP rule for this group.

03



Ghost Redemption

We identified a fake account pattern used for mileage abuse. A simple pattern-based reject rule was sufficient to completely stop the fraud.

04



Mileage Sale Abuse

We detected organized mileage sale activity originating from East Asia. We implemented a geo-specific reject rule that effectively blocked the abuse.

When we look at all these cases together, one thing is clear: We are no longer just monitoring fraud. We are preventing it — **in real time.**



Key Takeaways



Our Prediction Was Correct

Risks in the FFP ecosystem are increasing rapidly. Attacks are becoming significantly more organized and sophisticated.



Behavioral Signals Matter

Behavioral patterns are critical — both at the account level and transaction level.



Protection Without Friction is Possible

We proved that well-designed rules can effectively protect accounts while maintaining excellent customer experience and zero negative impact on the business.



Device Fingerprinting is Essential

Strong device fingerprinting performance is a cornerstone of effective defense. If it is weak, your entire security posture is compromised.



Real-World Validation

We successfully tested our system during a real large-scale attack — and it proved its value.



Velocity Rules — A Game Changer

Our dynamic, velocity-based rules capability delivers powerful real-time protection.



Intelligent Linking & Blacklisting

The ability to detect, link, and automatically blacklist suspicious elements (IP, Device, Account ID, etc.) has become another major game changer.



Rule-Based Security is Now Essential

A well-designed, rule-based account security system is no longer a “nice-to-have” — it is a business-critical necessity as risks continue to rise.



Key Remaining Elements

Key Remaining Elements

To Complete Our Advanced Account Security Project

SignUp Integration

Integration of registration flows is nearly complete.



Login Flow Issue

Reject action is not functioning properly in login flows.
Analysis completed; fix expected within the next few weeks.



Digital Behavioral Signals

Digital behavioral signals are ready for analysis. Expected to significantly boost detection accuracy once integrated.



Deep Account Behavioral Signals

Deep account-level behavioral signals are queued for analysis. Will deliver a major boost to our detection capability.



Other Integrations

Completion of the remaining integrations — including selected spending flows and retro-earning flows — will finalise the project and bring our Advanced Account Security capabilities to full maturity.



Our Vision & Expected Impact By 2027



With the successful completion of all remaining developments and integrations in our roadmap, we will achieve one of the highest levels of account protection in the industry. We expect a remarkable reduction in fraud volumes by 2027.



Ghost
Redemptions



%90



BOT Activities



%95



ATO
Redemptions



%90

These projections are based on our detailed analysis of current fraud patterns and methods. We know the attackers will never stop. They will continue evolving with new and more sophisticated techniques. But we will be ready. We will be on the battlefield — stronger, faster, and far more proactive.





Our AI-Powered Security Roadmap

With the completion of our current initiatives, we are now entering the next phase: building a more intelligent, proactive, and AI-supported account security ecosystem..



Rule Optimization

Training AI on our internal rule-writing logic to generate more optimal and scalable rules.



Categorization of Customer Cases

Using AI to analyse fraud cases, categorise them, identify trends, and deliver actionable insights.



Early Detection

Leveraging AI to monitor anomaly dashboards and instantly alert us to suspicious spikes and patterns.

Review of outcomes And deciding for the next step

Define the goals, budget, and project schedule before starting.



Preparation

Execute the project according to the plan and monitor progress.



Execution

Allocate resources and the team that will work on the project.



Approval

Regularly track project progress to ensure goals are met.



Defining The scope

Complete all deliverables and conduct project evaluation.





Turkish Airlines

Thanks :)