Case Study

TSYS
A Global Payments Company

TSYS Customer Success Story

How using non-monetary events in model scoring helps issuers to reduce fraud, increase authorizations and deliver exceptional customer experiences

Online businesses face unique challenges when managing card declines. When customers transact online, a payment provider will send the details of a charge through a card network like Visa or Mastercard to a customer's issuing bank as a payment request. The request, a message referred to as an ISO 8583, is encoded to include details like the cardholder's address, the transaction amount and business category.

While issuing banks use sophisticated reasoning to decide when to decline charges, there are 128 fields in the ISO 8583 message, and each issuing bank can choose how to interpret and combine them. Online authorization rates are often lower than in-person transactions because of the increased risk of unauthorized card use, even if it's a legitimate sale.

There are dozens of reasons payments can fail, from incorrect card information to a suspicion of fraud. Unfortunately, some consumers' genuine activity can look very similar to typical fraud which could have transactions wrongly declined. Not only does this lose issuers the interchange fees and interest they would have generated on those transactions, but when high-value customers are falsely rejected, issuers could lose their 'top of wallet' status as well. Ultimately wrong declines may taint a customer's relationship with both the merchant and issuer as they choose whether to take their business elsewhere.

While there is no way to eliminate network declines completely, forward thinking issuers and other financial institutions are utilizing machine learning to reduce false positives, fraud losses and unnecessary friction to customers.

> **33% of falsely-declined new shoppers abandon the transaction and retailer entirely and never try again.**
>
> *Sapio Research*

> **Merchants lose up to 75 times more revenue to false declines than they do to legitimate fraud ...**
>
> **62% of online merchants have seen false decline rates increase over the past two years.**
>
> *Aite Group*

Enhanced data driven insights enable seamless and secure assessment of transactions

In 2016, TSYS collaborated with Featurespace in a joint partnership to develop Foresight Score℠ to provide issuers with greater accuracy and efficiency in detecting fraud while maintaining high levels of customer experience.

The real-time fraud and risk scoring tool utilizes proprietary machine learning to profile genuine individual customer interactions in real time, understanding risk even as underlying behaviors change.

Foresight Score delivers enhanced data driven insights, facilitating simultaneous non-monetary events scoring. This enables seamless and secure assessment of transactions as the slightest deviations and anomalies in customer behavior are rapidly understood, evaluated, and acted on to stop fraud while allowing genuine customers to transact.

Using non-monetary account activity for model learning

Having additional information helps to determine if activities are genuine or fraudulent. In many cases issuers may not be using the score on this additional data as other scoring systems may not score at all. TSYS Foresight Score uses non-monetary account events for model learning order to place a better, more intelligent score on monetary purchase authorization in real time to spot anomalies and to catch fraud.

Use Cases

Non-Authorized Debit

Record Type 130 (Message Type)

EVENT USE CASE: Offline authorizations: payment system is not available at Point of Sale

Legitimate instance: A customer uses their credit card on a terminal which is offline such as on an airplane, train or a parking service.

Illegitimate instance: A fraudster finds a card and uses it at terminals which operate offline. Since major checks are not being conducted, cards can be used until a payment comes online and updates are made to the available balance.

Card Details

Tran Type 38 (Request Type)

EVENT USE CASE: A PIN number change (not a PIN order) or a balance inquiry

Legitimate instance: A customer checks their balance before withdrawing money.

Illegitimate instance: A fraudster steals a card and checks the balance before withdrawing money.

Registration

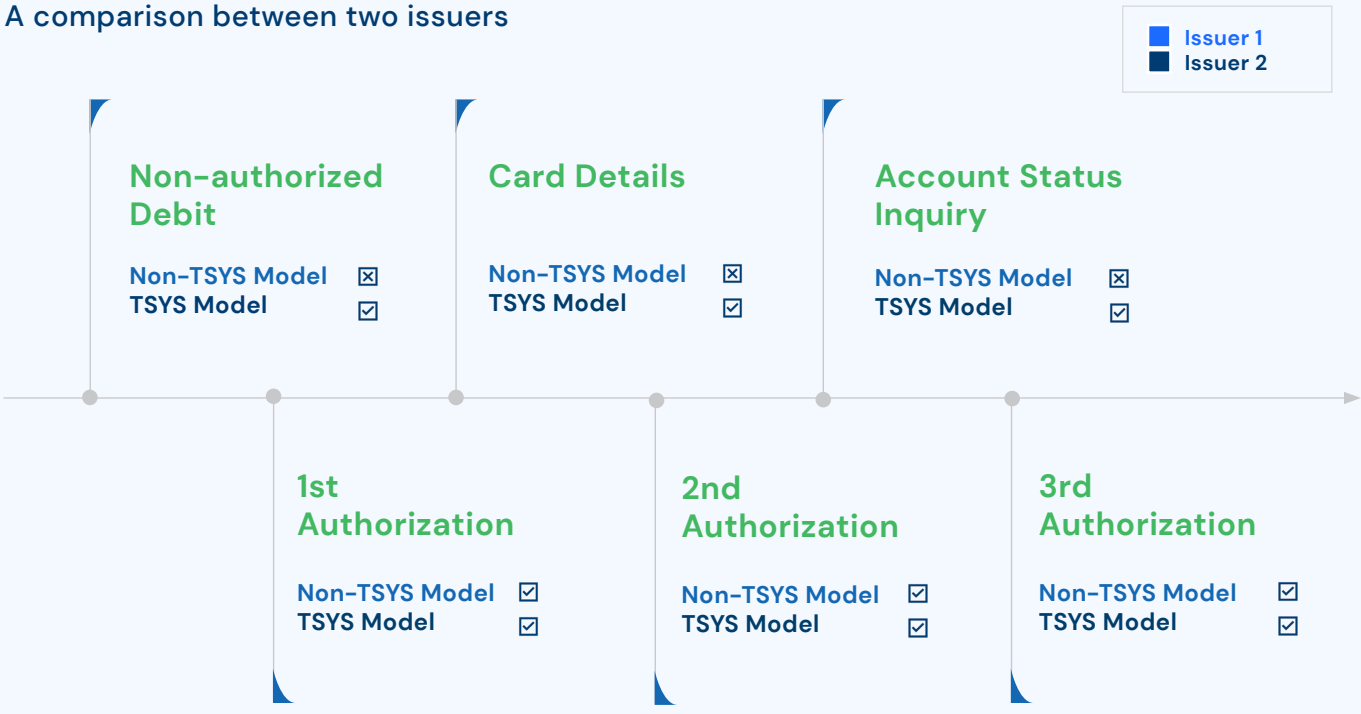
ASI 85 (Response Code) - $0 value auth

EVENT USE CASE: An online purchase

Legitimate instance: Tesco pings a customer's card for validity, as most often this will be a Card-Not-Present authorization.

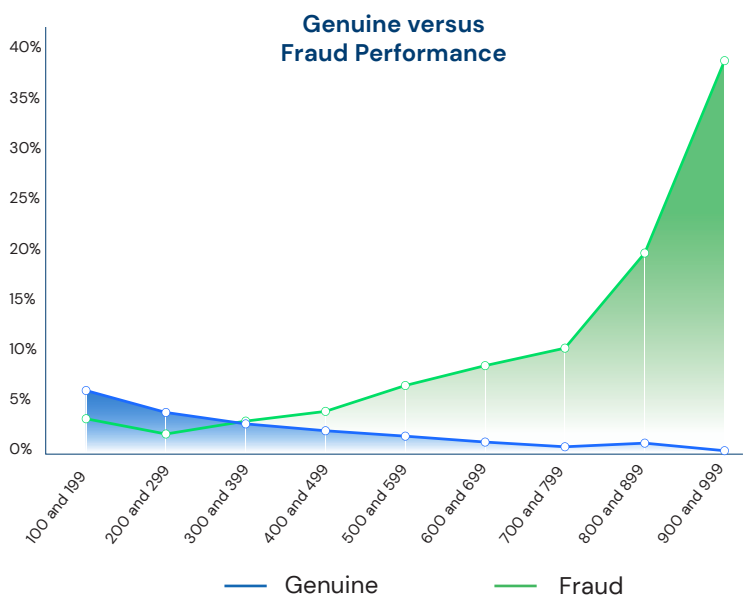
Illegitimate instance: A fraudster tests a range of cards on an unsuspecting company's website to determine which cards are active.

A comparison between two issuers



Additional non-monetary events are not necessarily transaction-based.

The graph below shows the performance comparison between genuine purchase transactions versus fraudulent transactions after non-monetary event scoring by the issuer with the TSYS Model.



Overall	
Accounts	
Genuine	750,542
Fraud	1,310

Overall approved	
Accounts	
Genuine	704,991
Fraud	1,038

Additional messages that would have been scored by the TSYS Model

Accounts	
Genuine	379,626
Fraud	392

Accounts	
Genuine	379,626
Fraud	392

Additional benefit	
Accounts	
Genuine	51%
Fraud	30%

Additional benefit	
Accounts	
Genuine	54%
Fraud	38%

Within 1,310 accounts, 30% had at least one additional message enabling more trigger points to write more effective rules to catch fraud earlier. By this evidence, using non-monetary events to enhance model learning is assisting in achieving the increase in overall fraud detected.

Issuer without TSYS Model

Additional Message Volumes				
	Transactions	Distinct Account	Amounts	Transactions/Accounts
Confirmed Genuine	1,500,000	380,000	£140,200,000	
Confirmed Fraud	850	400	£5,150	2.14

Authorization amount

£600
Loss per account

Additional Message Volumes - Approved Performance					
	Transactions	Distinct Account	Amounts	Transactions/ Accounts	Amounts/ Accounts
Confirmed Genuine	25,000,000	750,000	£1,250,200,000		
Confirmed Fraud	6,100	1,300	£780,000	4.68	£600

Authorization amount

Gross value in currency £

4.6
Authorizations per account

The issuer with no TSYS Foresight Score model has higher fraud losses and additional overhead costs having to manage the higher levels of fraud.

Issuer with TSYS Model

Additional Message Volumes				
	Transactions	Distinct Account	Amounts	Transactions/Accounts
Confirmed Genuine	10,000,000	2,470,000	£2,900,000,000	
Confirmed Fraud	6,250	4,100	£150,000	1.52

Authorization amount

£227
Loss per account

Additional Message Volumes - Approved Performance					
	Transactions	Distinct Account	Amounts	Transactions/ Accounts	Amounts/ Accounts
Confirmed Genuine	390,000,000	3,000,000	£3,567,500,000		
Confirmed Fraud	17,000	6,600	£1,500,500	2.58	£227

Authorization amount Gross value in currency £

2.5
Authorizations per account

The non-monetary events that Foresight scores: offline authorizations, card details, and account status inquiries emphasizes the performance with these additional messages, without impacting genuine customer transactions. Non-monetary event scoring assists the TSYS model in seeing fraud at higher bands without slowing down transactions on lower bands.

The power of additional non-monetary events

- Aids fraud analysts in more effective rule-writing by generating more trigger points
- Detects fraud earlier in the process, reducing overall fraudulent accounts and activity
- More fraud blocked and losses reduced
- More transactions processed and customer friction reduced
- Reduces operational costs to issuer fraud and customer support teams
- Increases customer trust

FEATURE SPACE
OUTSMART RISK

TSYS
A Global Payments Company