



## AI Fraud Score

---

Effectively protect your business against fraud with the self-learning transaction scoring solution from Computop.

# Contents

- 1 AI Fraud Score at a glance  
Page 4
- 2 How it works  
Page 6
- 3 Why do I need AI Fraud Score?  
Page 9
- 4 How do I integrate  
AI Fraud Score into Computop Paygate?  
Page 12
- 5 Coming soon: AI Fraud Score  
for other payment methods  
Page 14

# You wouldn't judge someone based on a single trait...

## ...and neither should your fraud protection solution!

Static risk assessments have proven to be a reliable protection against many credit card fraud schemes in online retail. However, they entail two major disadvantages:

- Trustworthy shoppers are sometimes rejected, simply because they are placing an order from a specific location or because their credit card was issued in a specific country.
- All new fraud patterns need to be defined manually. This means that newly emerging threat scenarios cannot be detected by static, rule-based scoring systems.

With Computop's AI Fraud Score, your risk management is no longer restricted to rigid exclusion criteria and generalizations of whole customer groups.

Fully integrated into Computop Paygate, AI Fraud Score is easy to configure and offers maximum protection against credit card fraud.

## How your business benefits from AI Fraud Score:



Gives you the ability to reach out to all relevant customers, as specific groups of sales prospects are no longer inherently excluded from your online sales.



Dynamic, selflearning risk scoring demonstrably reduces the number of fraudulent transactions mistakenly rated as uncritical.



With more customers and lower fraud rates, AI Fraud Score helps boost revenue and lower operational costs for credit card processing.

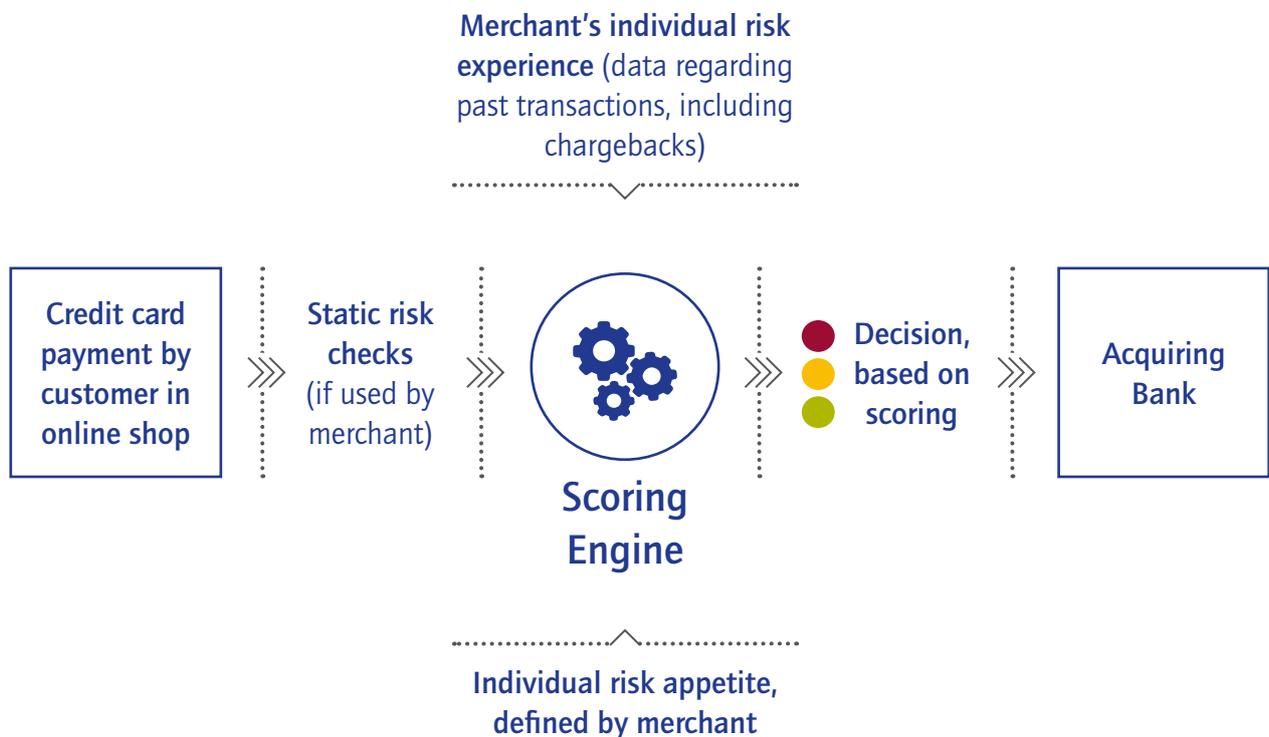
# 1 AI Fraud Score at a glance

## What's behind AI Fraud Score?

Computop AI Fraud Score is an automated risk scoring engine based on a self-learning computer algorithm. In addition to using Computop's established fraud checks, this new scoring technology relies on a broader range of risk parameters and automatically learns from merchants' chargeback and fraud histories.

Instead of simply weighing scores for single risk parameters, AI Fraud Score determines which constellation of parameters typically lead to fraud and chargebacks, and continuously adapts the scoring results to current fraud schemes and threat scenarios.

## How is AI Fraud Score used in the payment flow?



## Features of AI Fraud Score



### Machine learning approach

AI Fraud Score continuously learns from new chargeback data and adapts its scoring algorithm accordingly. As a result, the number of successful fraud attempts continues to decrease over time.



### Fully integrated in Computop Paygate

AI Fraud Score does not operate as a separate solution, but rather is fully integrated in CT Paygate. Simply activate it and adjust it to your business model and preferences to start using it.



### Adaptable to your individual fraud experience

Fraud likelihoods vary among merchants depending on their target markets, target groups and product assortments. AI Fraud Score's algorithm is adjusted to your prior fraud experience right from the start.



### Customizable to your individual risk appetite

AI Fraud Score lets you decide how to deal with ambiguous credit card transactions by defining your own risk thresholds for scoring results and purchase amounts.



### Compliant with the new EU Geoblocking Regulation

AI Fraud Score does not generally block IP addresses and BINs based on their country of origin. Transactions are only rejected if a characteristic fraud pattern emerges from all available data points.



### Try it out for free before going live

Want to know how AI Fraud Score's transaction risk analysis will impact your conversion rates? Simply put it to the test completely free of charge. During your trial period, AI Fraud Score will analyze your transactions and generate risk scores without actively intervening.

## 2 How it works

### Payment data used in the scoring engine

In order to calculate the fraud probabilities of incoming credit card payments, AI Fraud Score uses data from your past transactions. For this purpose, our scoring engine collects and analyzes data points that are able to indicate possible fraud attempts.

Transaction amount	Time of transaction	Issuer country – IP country match (same origin)
Issuer BIN (Country in which the card was issued)	Is an IP-anonymizer being used to make the online purchase?	Velocity checks: frequency of use of card number, IP address, email address and device
IP address (Country and region of purchase)	Billing address	Shipping address

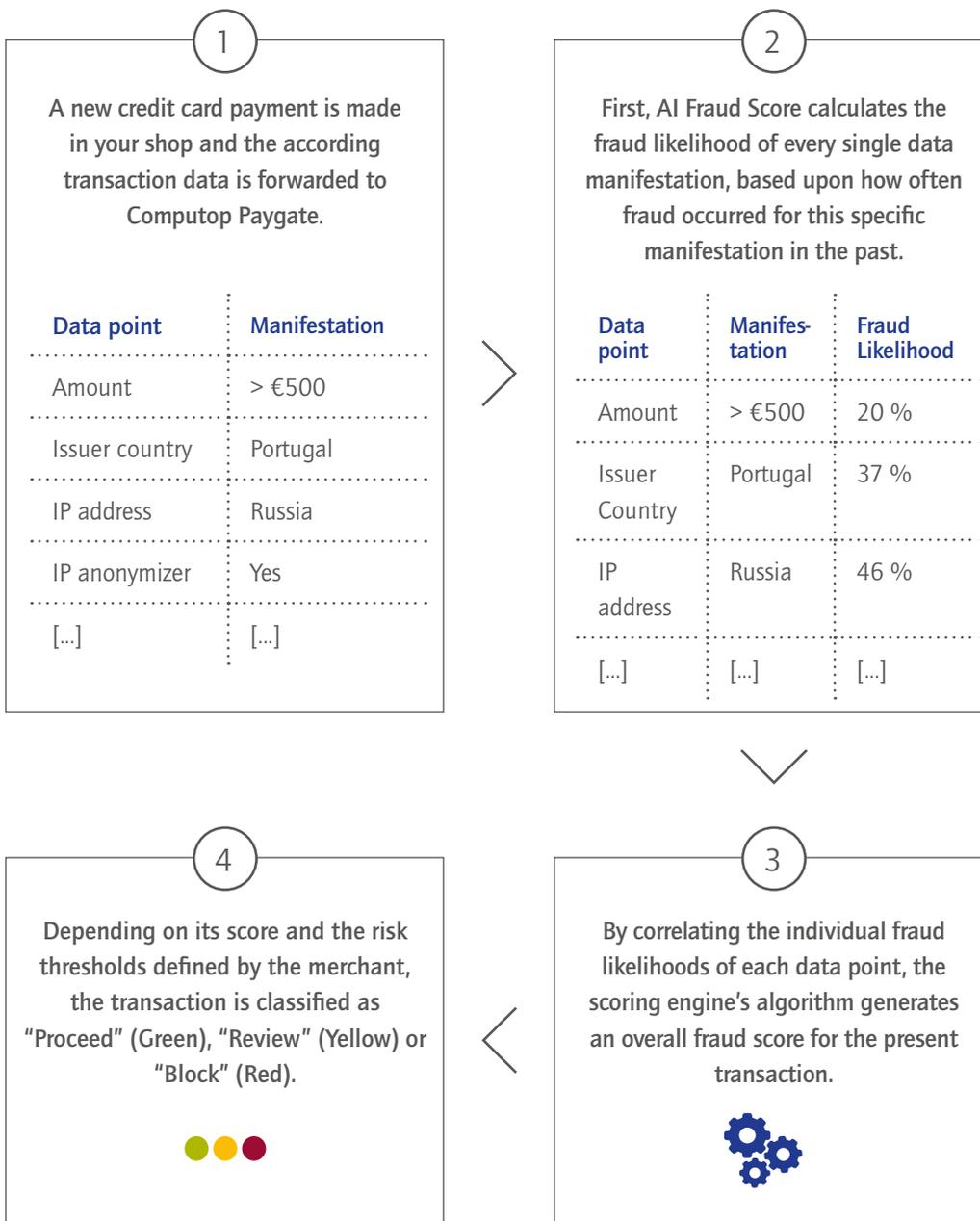
#### Good to know:

AI Fraud Score's scoring engine does not make decisions based on strict knock-out criteria (as used in rule-based, static risk checks). For instance, a purchase made at a suspicious time of day from a suspicious country is not necessarily disqualified if all other data points indicate the purchase is not fraudulent.

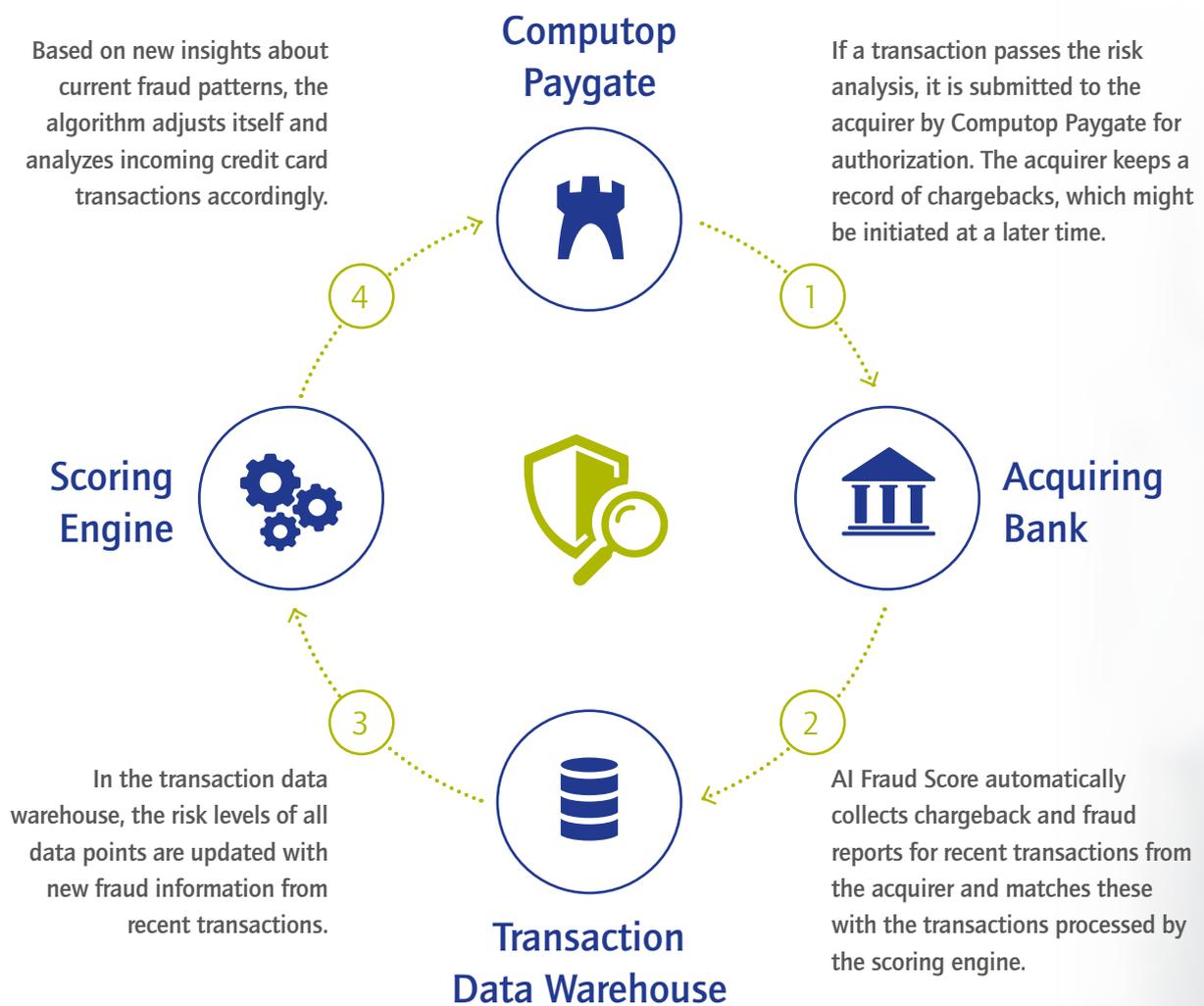
If you already use CT Paygate, you do not need to make any changes to your existing setup. As per the mandatory requirements laid out by the EMVCo 3D Secure 2.0 protocol for online credit card processing, Computop already collects the transaction data in question and subsequently transmits it to the cardholder's issuing bank.

## The algorithm: how scores are calculated

Our scoring engine's logic is based on a recognized approach in probability calculation that has proven its predictive accuracy, particularly in machine learning environments. The diagram below demonstrates the process flow:



## AI Fraud Score automatically adjusts its scoring to the latest findings from current transactions and improves its analysis results every day.



## ③ Why do I need AI Fraud Score?

### My business has been doing well with static, rule-based risk checks. Why change?

Static risk checks (such as those that reject transactions from certain countries) have been doing a good job of helping online merchants prevent credit card fraud. And in many scenarios, selected fixed rules are still a reasonable solution. Nevertheless, there are clear disadvantages to using rule-based risk checks:

- They are subjective. The configuration of a rule-based fraud prevention tool is executed by fraud analysts with individual knowledge and opinions.
- They require constant human monitoring and quickly become obsolete due to the constant evolution of fraud schemes.
- They only consider easy correlations, since it is difficult for humans to think in more than three dimensions and therefore explore complex pattern combinations.
- They can only detect known fraudulent strategies.

#### Good to know:

AI Fraud Score does not need to completely replace established risk settings in CT Paygate. If you are pleased with the results that certain static risk checks have been providing, both approaches can be easily combined.



## The new 3D Secure 2.0 protocol already provides risk scoring based on multiple transaction data points. What is the added value of AI Fraud Score?

With effect as of September 2019, the processing of credit card transactions in the European Economic Area is subject to the 3D Secure 2.0 protocol. This includes real-time transaction risk analysis (conducted by the issuing banks) for online credit card payments. However, for various reasons, the 3D Secure 2.0 risk analysis cannot replace risk management controlled by the merchant.



## Higher accuracy of individualized transaction risk analysis compared to 3D Secure 2.0

Transactions that prove fraudulent despite passing the 3D Secure 2.0 assessment will become more common in the future. Since the transaction risk analysis employed by issuers does not consider a merchant's individual fraud history and business model, certain fraud patterns may be overlooked by their screening tools.

## Out of scope for 3D Secure 2.0: "one leg out" transactions

If the buyer (the issuing bank) or the merchant (the acquiring bank) are located outside the European Union, 3D Secure 2.0 does not apply.

## Out of scope for 3D Secure 2.0: MOTO transactions

When fraud becomes more difficult in one channel, fraudsters will likely migrate to another: merchants active in MOTO channels (Mail Order/Telephone Order) should stay alert to increased fraud and use a risk analysis tool they can manage themselves, since credit card payments made via these channels are not covered by 3D Secure 2.0.



## Use Case „one leg out“: international e-sales

Merchants that generate a high share of revenue abroad and do not use a fraud analysis solution of their own encounter a large number of transactions passing through payment processing without appropriate fraud screening.



## Use case MOTO 1: classic mail order business

Especially in markets with a high share of elderly consumers, the option of ordering via mail is an essential requirement for retailers. However, a credit card payment initiated by letter order does not pass through the 3D Secure 2.0 procedure.



## Use case MOTO 2: ticket sales via phone order

If your business is hosting events and selling tickets, many customers may still expect you to offer the option of ordering via phone. Also, credit card payments by phone are not protected by 3D Secure 2.0.

# 4 How do I integrate AI Fraud Score into Computop Paygate?

## What merchants need to do

As a native component of Computop Paygate, AI Fraud Score merely needs to be activated and configured to begin working. There's no additional programming required on your part.

### Start a free trial:

We offer a free trial of AI Fraud score to ensure it provides the best possible protection for your business before going live. In addition to your existing risk checks, the scoring engine will scan your credit card transactions and generate scores for them, but will remain idle. At the end of the trial, simply compare the results to see how it performed.

- 1 Activate AI Fraud Score:**  
Let your account manager or technical support agent know that you would like to start a trial.
- 2 Set initial fraud likelihoods (page 9)**  
for credit card transaction parameters. This can be done in two ways:
  - Based on your prior transaction data
  - If you are a new Computop customer, fraud likelihoods will be set based on your estimate and the assessment of our fraud experts
- 3 Define your individual risk appetite (page 9)**
  - By determining scoring thresholds for each available action (approval, revision, rejection)
  - By defining different risk classes depending on the transaction amount

### Go Live:

- 4** Before going live, we'll take a look at your existing static risk checks to help you decide whether to keep some of them or to have them replaced entirely by the scoring engine logic.

# How to configuring the scoring engine

**Figure 1**

Define individual fraud likelihoods for credit card transaction parameters:

Probabilities of Fraud based on Data Points

Transaction Amount

BIN country

Active

Regions	% Fraud	% Legitimate	Country
	35	86	Austria, Germany, Switzerland
	10	1	Algeria, Ukraine

	% Fraud	% Legitimate
Unknown	50	50
Other	8	1

IP country

BIN - IP country relationship

IP Anonymizer

Active

	% Fraud	% Legitimate
Used	11	1
Not used	89	99

**Figure 2**

Define your individual risk appetite by setting individual scoring thresholds for eligible actions (approval, review, rejection) as well as for different buy amounts.)

Decision Maker

Caps on Fraud Probability % for actions

Active

Result data in Response

Up to Amount / Currency	Level 1	Level 2	Currency
	50	150	EUR
	100	200	GBP

	Level 1	Level 2	Above	Traffic Light
Proceed without 3DS up to	30	25	20	●
Proceed with 3DS up to	50	45	40	●
For review up to	75	70	65	●

# 5 Coming soon: AI Fraud Score for other payment methods

## Intelligent fraud prevention for all relevant payment methods

AI Fraud Score is a powerful tool in the fight against credit card crime. It provides higher conversion rates, more revenue and continuously decreasing rates of fraud for merchants.

More good news: self-learning fraud prevention is effective for more than just protecting your credit card transactions. Computop's latest generation of risk management solutions will be based exclusively on artificial intelligence and will include fraud protection coverage for other popular, at-risk payment methods.

### Coming Soon:

- > AI Fraud Score for purchase on account
- > AI Fraud Score for direct debit

## Payment & AI: Stay up to date!

Artificial intelligence opens up undreamed-of potential for the payment industry. As a merchant, you can look forward to offering your customers an even better payment experience in the future – as well as saving time and money.

Computop's payment people have been fascinated by AI research since the very start. With passion and expertise, we are constantly improving our products to provide our customers with the best tools for processing customer payments on all channels worldwide, even in the payment world of tomorrow.

Interested in artificial intelligence? Want to learn more about how this new technology will affect retail? Get in touch with us to begin a stimulating exchange of ideas!



## Challenge us

Have questions? Ask us! The Payment People from Computop are here to answer your questions. We will work with you to find the best individual payment solution for your business. New and demanding challenges welcome!

Here's how to reach us:

DE T: +49 (0) 951-98009-22  
sales@computop.com

UK T: +44 (0) 1932 895735  
uk@computop.com

USA T: + 1 800 701 7806  
usa@computop.com

CHINA T: +852 2918-8295  
china@computop.com