

Fraud prevention

- [About Fraud prevention with IP tracking](#)
 - [General information about Fraud prevention](#)
- [Additional parameters for Fraud prevention](#)
 - [Definitions](#)
 - [Data formats](#)
 - [Abbreviations](#)
 - [Additional parameters for calling Computop Paygate interface for credit cards](#)
 - [Calling the interface for editing a Blacklist](#)
 - [BlackListInfo](#)

About Fraud prevention with IP tracking

General information about Fraud prevention

Computop Paygate supports different processes for fraud prevention. These include inquiries with credit agencies for the monitoring of the card's country of origin and payment guarantees for credit cards.

A large proportion of fraud attempts come from foreign countries. Computop Paygate can check the country of origin and, in many cases the city of the IP address used. If the country of origin or the IP address of your customer is not one of your supplies countries or is not the same country as the credit card Issuer, Computop Paygate can send an alert via e-mail or automatically refuse the payment.

75% of all fraud attempts are made with foreign credit cards. Computop Paygate can check the card's origin: If you enter the delivery country as a parameter, Computop Paygate returns the country of origin of Visa and MasterCard issued cards and sends an e-mail if the delivery country differs from the card's origin. You can then find out from the customer why the card's origin differs from the delivery country to avoid fraud. Computop Paygate can optionally refuse such payments immediately.

Additional parameters for Fraud prevention

Definitions

Data formats

Format	Description
a	alphabetical
as	alphabetical with special characters
n	numeric
an	alphanumeric
ans	alphanumeric with special characters
ns	numeric with special characters
bool	boolean expression (true or false)
3	fixed length with 3 digits/characters
..3	variable length with maximum 3 digits/characters
enum	enumeration of allowed values
dtm	ISODateTime (YYYY-MM-DDThh:mm:ss)

Abbreviations

Abbreviation	Description	Comment
CND	condition	

M	mandatory	If a parameter is mandatory, then it must be present
O	optional	If a parameter is optional, then it can be present, but it is not required
C	conditional	If a parameter is conditional, then there is a conditional rule which specifies whether it is mandatory or optional

Notice: Please note that the names of parameters can be returned in upper or lower case.

Additional parameters for calling Computop Paygate interface for credit cards

Fraud prevention via IP-tracking relates to VISA and MasterCard credit cards via Computop Paygate interfaces [payssl.aspx](#), [paynow.aspx](#) and [direct.aspx](#).

For standard integration and other special parameters for making a credit card payment via the [payssl.aspx](#), [paynow.aspx](#) and [direct.aspx](#) interfaces, please check the credit card handbook.

Notice: By default the fraud prevention functions are not activated. [Computop Sales](#) can activate these functions for you if required.


Notice: For security reasons, Computop Paygate rejects all payment requests with formatting errors. Therefore, please use the correct data type for each parameter.


The following table describes the [encrypted payment request parameters](#):

Key	Format	CND	Description
IPAddr	ans..15	O	IP address. If you transfer the IP address, Paygate can determine in which country and in which town your customer has connected with the Internet (see also IPZone). Format: 123.456.789.012
IPZone	ans..1100	O	Codes of countries from which you accept orders, 3 digits numeric according to ISO 3166-1. Separate several countries by commas: 036,040,124 . If you transmit countries in IPZone , Paygate checks the country of origin of your customer's IP address, whether it is included in your country list, and whether it corresponds to the country of the credit card (see below). Paygate also transmits the IP-country to your shop (see below). If the IP-country is not in your list or does not match the credit card Paygate can send a warning e-mail or refuse payments.
Zone	ans..1100	O	Codes of countries where you accept credit cards, 3 digits numeric or alphanumeric according to ISO 3166-1. Separate several countries by commas: 036,040,124. If you transmit countries in Zone, Paygate checks the country of origin of your customer's credit card (MasterCard, Visa) and whether it is included in your approved country list. Paygate also transmits the card's country to your shop (see below). If the card's-country is not in your list or does not match your customer's IP address, Paygate can send a warning e-mail or refuse payments. In order to refuse cards from particular countries (negative list) enter an exclamation mark before that country code: !036,!040,!124. Please note, there is a maximum length of 1100 characters.

Additional parameters for Fraud prevention for credit card payments

The following table describes the result parameters with which the Computop Paygate responds to your system

 pls. be prepared to receive additional parameters at any time and do not check the order of parameters

 the key (e.g. MerchantId, RefNr) should not be checked case-sensitive

Key	Format	CND	Description
Zone	a..7	O	If country codes have been entered in Zone Paygate returns the country code for the credit card or "UNKNOWN"
IPZone	a..7	O	If IP-countries are transmitted in IPZone in the case of the inquiry Paygate returns the country code of the IP address or "UNKNOWN"
IPZoneA2	a..7	O	If IPZone is submitted within the request Paygate returns the two-character country code of the IP address or "UNKNOWN" (DE=Germany, FR=France etc.)
IPState	a..32	O	If IPZone is submitted in the request Paygate returns the federal state from which the IP address of your customer originates.
IPCity	a..32	O	If IPZone is submitted in the request Paygate returns the town/city from which the IP address of your customer originates.
IPLongitude	n..20	O	If IPZone is submitted in the request Paygate returns the geographical longitude (floating point, decimal) of the dial-in node (PoP) of your customer.
IPLatitude	n..20	O	If IPZone is submitted in the request Paygate returns the geographical latitude (floating point, decimal) of the dial-in node (PoP) of your customer

fsStatus	ans..9	OC	Only via direct.aspx, only with EVO Payments International: ACCEPT=no suspicion of card fraud, DENY=refusal recommended, CHALLENGE= verification recommended, NOSCORE=No risk analysis, ENETFP=Exceptional error in the network, ERROR=Error in the data processing centre, ETMOUT=Timeout
fsCode	n4	OC	Only via direct.aspx, only with EVO Payments International: Recommended action: <0000> no result, <0100> accept, <0150> always accept, <0200> deny, <0250> always deny, <0300> suspicious, <0330> please check, <0400> suspicious ReD blacklist, <0500> questionable, <0600> questionable ReD blacklist, <0700> threshold exceeded, <0800> unusual usage, <901> intern ebitGuard error, <902> format error

Additional response parameters for fraud prevention for credit card payments

Calling the interface for editing a Blacklist

In order to create, read, update or delete a blacklist entry via a Server-to-Server connection, call the following URL:

<https://www.computop-paygate.com/BlackList.aspx>

Notice: For security reasons, Computop Paygate rejects all payment requests with formatting errors. Therefore, please use the correct data type for each parameter.

The following table describes the [encrypted payment request parameters](#):


Key	Format	CND	Description
MerchantID	ans..30	M	MerchantID, assigned by Computop. Additionally this parameter has to be passed in plain language too.
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <ul style="list-style-type: none"> HMAC Authentication (Request) HMAC Authentication (Notify)
EventToken	enum	M	Abbreviation of the action to be done: <Create>, <Read>, <Update> or <Delete>
BlackListInfo	ans..1024	M	Information about the blacklist entry as JSON string in the Base64 format. See table BlackListInfo below.


Key	Format	CND	Description	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <ul style="list-style-type: none"> HMAC Authentication (Request) HMAC Authentication (Notify) 	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: <ul style="list-style-type: none"> HMAC-Authentisierung (Anfrage) HMAC-Authentisierung (Notify)

Key	Format	CND	Description	Beschreibung
EventToken	enum	M	Abbreviation of the action to be done: <Create>, <Read>, <Update> or <Delete>	Abkürzung der auszuführender Aktion: <Create>, <Read>, <Update> oder <Delete>
BlackListInfo	ans..1024	M	Information about the blacklist entry as JSON string in the Base64 format. See table BlackListInfo below.	Information über den Blacklist-Eintrag als JSON-String im Base64-Format. Siehe Tabelle BlackListInfo unten.

Parameters for calling the blacklist editing

The following table describes the result parameters with which the Computop Paygate responds to your system

 pls. be prepared to receive additional parameters at any time and do not check the order of parameters

 the key (e.g. MerchantId, RefNr) should not be checked case-sensitive

Key	Format	CND	Description
mid	ans..30	M	MerchantID, assigned by Computop

MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <ul style="list-style-type: none"> HMAC Authentication (Request) HMAC Authentication (Notify)
Status	a..50	M	OK (URLSuccess) or FAILED (URLFailure)
Description	ans..1024	M	Further details in the event that payment is rejected. Please do not use the Description but the Code parameter for the transaction status analysis!
BlackListInfo	ans..1024	C	Information about the blacklist entry as JSON string in the Base64 format, if Status=OK. See table BlackListInfo below.

Key	Format	CND	Description	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <ul style="list-style-type: none"> HMAC Authentication (Request) HMAC Authentication (Notify) 	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: <ul style="list-style-type: none"> HMAC-Authentisierung (Anfrage) HMAC-Authentisierung (Notify)

Key	Format	CND	Description	Beschreibung
Status	a..50	M	OK (URLSuccess) or FAILED (URLFailure)	OK (URLSuccess) oder FAILED (URLFailure)

Key	Format	CND	Description	Beschreibung
Description	ans..1024	M	Further details in the event that payment is rejected. Please do not use the Description but the Code parameter for the transaction status analysis!	Nähere Beschreibung bei Ablehnung der Zahlung. Bitte nutzen Sie nicht den Parameter Description , sondern Code für die Auswertung des Transaktionsstatus!

Key	Format	CND	Description	Beschreibung
BlackListInfo	ans..1024	C	Information about the blacklist entry as JSON string in the Base64 format, if Status=OK. See table BlackListInfo below.	Information über den Blacklist-Eintrag als JSON-String im Base64-Format, wenn Status=OK. Siehe Tabelle BlackListInfo unten.

Result parameters for calling the blacklist editing

BlackListInfo

Following table describes the BlackListInfo object for EventToken Insert:

Key	Format	CND	Description
Category	enum	M	Category <EDD> for direct debit or <CC> for credit card
Number	ans..64	M	IBAN, if Category=EDD Credit card number, if Category=CC
BIC	ans..32	C	BIC, if Category=EDD

Parameters for blacklist editing, EventToken Insert

Following table describes the BlackListInfo object for EventToken Update:

Key	Format	CND	Description
BlockID	an..32	M	Unique BlockID
LockActive	bool	M	Defines, if the entry should be blocked or not. Blocked: <True> Unlocked: <False>

Parameters for blacklist editing, EventToken Update

Following table describes the BlackListInfo object for EventToken Delete:

Key	Format	CND	Description
BlockID	an..32	M	Unique BlockID

Parameters for blacklist editing, EventToken Delete

The following table describes the BlackListInfo object with which the Computop Paygate responds:

Key	Format	CND	Description
BlockID	an..32	M	Unique BlockID
mid	ans..30	M	MerchantID, assigned by Computop
Category	enum	M	Category <EDD> for direct debit or <CC> for credit card
Number	ans..64	M	IBAN, if Category=EDD Credit card number, if Category=CC
BIC	ans..32	C	BIC, if Category=EDD
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <ul style="list-style-type: none"> HMAC Authentication (Request) HMAC Authentication (Notify)
LockActive	bool	M	Defines, if the entry should by blocked or not. Blocked: <True> Unlocked: <False>
Created	dtm	M	Time of creation (YYYY-MM-DD hh:mm:ss)
Changed	dtm	M	Time of modification (YYYY-MM-DD hh:mm:ss)

Key	Format	CND	Description	Beschreibung
mid	ans..30	M	MerchantID, assigned by Computop	HändlerID, die von Computop vergeben wird

Key	Format	CND	Description	Beschreibung
Category	enum	M	Category <EDD> for direct debit or <CC> for credit card	Kategorie <EDD> für Lastschrift oder <CC> für Kreditkarte
Number	ans..64	M	IBAN, if Category=EDD Credit card number, if Category=CC	IBAN, wenn Category=EDD Kreditkartennummer, wenn Category=CC
BIC	ans..32	C	BIC, if Category=EDD	BIC, wenn Category=EDD

Key	Format	CND	Description	Beschreibung
MAC	an64	M	Hash Message Authentication Code (HMAC) with SHA-256 algorithm. Details can be found here: <ul style="list-style-type: none"> HMAC Authentication (Request) HMAC Authentication (Notify) 	Hash Message Authentication Code (HMAC) mit SHA-256-Algorithmus. Details finden Sie hier: <ul style="list-style-type: none"> HMAC-Authentisierung (Anfrage) HMAC-Authentisierung (Notify)

Key	Format	CND	Description	Beschreibung
LockActive	bool	M	Defines, if the entry should by blocked or not. Blocked: <True> Unlocked: <False>	Definiert, ob der Eintrag gesperrt werden soll oder nicht. Gesperrt: <True> Entsperrt: <False>
Created	dtm	M	Time of creation (YYYY-MM-DD hh:mm:ss)	Zeit des Anlegens (YYYY-MM-DD hh:mm:ss)
Changed	dtm	M	Time of modification (YYYY-MM-DD hh:mm:ss)	Zeit der Änderung (YYYY-MM-DD hh:mm:ss)

Result parameters for blacklist editing