Fraud Detection Module (basic)

Table of contents

1. Introduction

In distance selling, the fight against fraud requires maximum levels of know-how, speed and flexibility. To help you implement effective risk management, the Fraud Detection Module offers a real-time service that provides all the necessary analysis information, and offers fully customised safeguards for handling dubious transactions.

Use of the Fraud Detection Module does not, however, guarantee protection against all fraud, it only helps you to thwart it. The Fraud Detection Module can be configured based on the risks or past fraud issues that have been encountered by your business.

1.1 Benefits

The Fraud Detection Module allows you to:

- Detect anomalies during transactions
- Immediately block attempts by recognised fraudsters
- Protect against country-specific risks
- Define and apply fully customised security policies
- Benefit from a conditional payment guarantee in accordance with your individual acquirer’s policies (3-D Secure)

1.2 Contents

The Fraud Detection Module comprises three separate functional areas:

- Fraud detection activation and configuration
- 3-D Secure
- Blacklist / whitelist / greylist

Important

- The VISA/MasterCard criteria described in this documentation are not necessarily available for all payment methods.

  The availability of “Activation and configuration” depends on the payment method. For some payment methods, the configuration is limited.

  We recommend that you check the specific selection criteria for your individual payment methods by clicking the “Edit” button next to the payment method in the “Fraud detection activation and configuration" table in your Fraud Detection Module.

- In **Batch** mode (file upload), only the following features of the fraud detection module are supported:
  - Blocking rules: Card country
  - Card blacklist
  - BIN blacklist

2. Activation and configuration

In the “Activation and configuration table you will see the distinction between credit cards and other payment methods.

The table contains blocking rules and optional limits. “No” indicates that nothing has been configured in the option page concerned. When a page has already been configured, the status will be “Yes”.

We shall now take a closer look at the configuration of fraud detection options for credit cards.

2.1 Blocking rules

Blocking rules become effective once the customer has entered his credit card details and has clicked the button to process the payment.

If the transaction does not comply with the rules you entered, we will retain the transaction and set its status to "Authorisation refused"

2.1.1 Card country

All card countries are accepted by default. Here, the term ‘card country’ means the country in which the card was issued. Our system can identify the card country based on the card’s BIN code. The BIN code is the first 6 digits of a credit card number. A BIN code is linked to a specific bank in a specific country.

If you want to set a list of countries, you can select them in the list on the right-hand side of the screen and click the “Add” button.

Above the list of selected countries you have the options to set your list to accepted countries (only accept payment from country list) or rejected countries (reject payment from country list).

2.1.2 IP address country

All IP address countries are accepted by default. Our system can identify the IP address country based on your customer’s IP address (although this check gives positive results in 94% of all cases, this IP check is based on externally provided IP listings, so there is a slight risk of error, as we rely on the accuracy of this list).

If you want to set a list of IP address countries, you can select them in the list on the right-hand side of the screen and click the “Add” button.

Note

The A1 (Anonymous proxy), AP (Asian Pacific region), EU (European network) and A2 (Satellite providers) codes refer to IP addresses for which the country of origin is uncertain.
EU, for example, means that the exact IP country is uncertain but it belongs to Europe. Accepting EU as IP address country does not mean you are accepting payments from all countries in Europe, it means you’re accepting payments from IP addresses managed by European institutions. If you want to accept payments from specific countries in Asia or Europe, you need to add the countries one by one to your list.
Anonymous proxies are internet access providers that allow internet users to hide their IP address. **We discourage you to accept payments originating from anonymous proxies!**

Above the list of selected IP address countries, you have the options to set your list to accepted countries (accept only payment from country list) or rejected countries (reject payment from country list).

You can always delete a country in the list by clicking the “Del” box in front of the country and then clicking on the “Submit” button below the list.

2.1.3 Country consistency

When you set this parameter to “Yes”, you will only allow transactions when the customer’s IP address is in the same country as his credit card issuer, in other words: only if the card country and IP address country are identical. This check is not performed if the IP address is from an anonymous proxy, the Asia Pacific network, the European network or a satellite provider.

2.1.4 3-D Secure

This parameter allows you to bypass the blocking rules set above if the cardholder is identified with 3-D Secure.

When a credit card is 3-D Secure and you have a 3-D Secure contract with your acquirer, you will have a conditional payment guarantee for the transaction. Even if you do not wish to receive payments from country X therefore, due to a high risk of fraud, you can still permit transactions with 3-D Secure credit cards from country X, as you do not have any risk regarding disputes over non-identification of the cardholder. (However, this does not apply to disputes over other matters).

2.2 Limits

2.2.1 Amount per transaction

You can limit the amount per transaction.

You can enter a minimum and a maximum amount. If the transaction amount is not within the limits you entered, we will retain the transaction and set its status to “Authorisation refused”.

The currency of the limit will be your main account currency. If you have multiple currencies and a transaction takes place in a currency other than your default one, our system will convert the limit into the other currency.

2.2.2 Card utilisation

You can set the “maximum utilisation per card, per period” based on the total amount of transactions per card and the number of transactions per card.

You have to configure this limit based on your business/products. If you sell a product that a person will not buy more than once a week, for instance, you can limit the card utilisation to 1 time per week.

Example

If you do not want to accept more than two transactions on the same day for a certain credit card and you do not want to accept more than 250 EUR on that credit card within that day, you could configure:

- Maximum utilisation per card, per period **1** day(s)
- Total amount of transactions per card: **250 EUR**
- Number of transactions per card: **2**

The “maximum utilisation per card, per period” limit only applies to cards that were used in transactions resulting in any of the following statuses: 9, 91, 92, 5, 51, 52

Note about "period"

If you enter the value "1" for the period, it covers the last 24 hours. However, if you enter “0” for the period, the period of the velocity check starts at midnight of the current day.

Example: For the date and time 2016/04/01 12:17 PM, the period starts at 2016/04/01 12:00 AM.

For the "current day", we use the time zone configured in your account.

3. 3-D Secure

3-D Secure offers a high level of security, as it allows customers to be identified unambiguously through technologies, e.g. html passwords, Digipass, card readers, biometrics, etc., implemented by the issuing banks.

By offering 3-D Secure, a merchant benefits from a conditional payment guarantee (see here), as described in the 3-D Secure contract with his acquirer. Under these conditions, a merchant's account is no longer debited for disputes over "non-identification of the cardholder". (This does not apply to disputes over other matters!)
The following brands have implemented the 3-D Secure protocol:

- Visa under the name of Verified by Visa
- MasterCard under the name of SecureCode
- JCB under the name of J-Secure
- American Express under the name of SafeKey

3.1 General

3.1.1 Affiliation request

If you click this “Request 3-DS” button, an email will be sent to your acquirer. If your contract with your acquirer does not provide for 3-D Secure, you can contact your acquirer for more information on registering for 3-D Secure, if you would like your acquirer to provide the 3-D Secure payment option.

Note: To enroll for SafeKey, please contact American Express or go to the SafeKey portal.

Once 3-D Secure has been enabled in your account you will see the activation date in the table. You can change the configuration for 3-D Secure by clicking the ‘edit’ button next to the payment methods.

3.1.2 Standard 3-D Secure transactions processing

1. When we receive the credit card details from your customer, our system sends a request to the VISA/MasterCard/JCB/AmEx directory to establish whether the card is registered, i.e. the cardholder has received some means of identification linked to his/her card and, if appropriate, gets the issuer authentication server data.
2. If the card is registered, our system redirects the customer to the issuer authentication server to initiate the authentication.
3. Our system receives the result of the authentication and processes the payment in the usual way.

If authentication is successful, the merchant can benefit from the conditional payment guarantee provided by his acquirer.

If the card is not registered, the merchant receives some level of conditional payment guarantee provided by his acquirer.

In both cases therefore, under certain conditions (defined by VISA, MasterCard and financial organisations, and as described in the 3-D Secure contract with his acquirer), the merchant has a payment guarantee, even without receiving identifying information from the customer. **These conditional payment guarantee rules are exclusively managed between the merchant and his acquirer. PostFinance only acts as a technical intermediary.**

3.2 Configuration options

The following are the configuration options for Verified by Visa, MasterCard SecureCode, J-Secure and SafeKey. Depending on your acquirer, some (or all) of these options might be inaccessible.

3.2.1 Technical problem

The merchant can choose to continue or interrupt the transaction, should a technical problem prevent connection to the VISA/MasterCard /JCB/AmEx directory during the 3-D Secure registration check.

If a technical problem prevents our system from connecting to the VISA/MasterCard/JCB directory (step 1), VISA/MasterCard/JCB/AmEx recommends that the process should be continued without authentication (continue option). In this case, however, the merchant will not benefit from the conditional payment guarantee.

3.2.2 Identification service temporarily unavailable

The merchant can choose to continue or interrupt the transaction, if the cardholder identification service is temporarily unavailable.

If the issuer authentication server is temporarily unavailable (step 2), cardholder identification is not possible. In this event, VISA/MasterCard/JCB/AmEx recommend continuing the process (continue option). In this case however, the merchant will not benefit from the conditional payment guarantee (see here).

3.2.3 Authentication fails (MasterCard only)

The merchant may choose to continue or interrupt the transaction, should the authentication fail.

Should cardholder authentication fail (step 3), MasterCard recommends interrupting the payment processing (interrupt option). If the transaction continues, the merchant will not benefit from the conditional payment guarantee (see here).

3.2.4 Activate/deactivate 3-D Secure

Here the merchant can switch on/off 3-D Secure for all VISA/MasterCard/JCB/AmEx cards.

Note: If 3-D Secure is disabled, the merchant will not benefit from the conditional payment guarantee (see here).

4. Blacklist / whitelist

In the Fraud Detection Module, you can generate your own blacklists for credit cards based on BIN codes, credit card numbers and IP addresses from which you do not wish to accept transactions, and a whitelist based on IP addresses.

“No” indicates that nothing has been configured in the blacklist/whitelist concerned. When a blacklist/whitelist has already been configured, the status will be “Yes”.

If, for a new transaction in your account, the BIN, credit card number or IP address has been entered on your blacklist, we will retain the transaction and set its status to “Authorisation refused”.

4.1 Credit Cards

There's no limit to the amount of entries per list.

You can add a comment to an entry in a blacklist or whitelist. You can enter it at the time of submission by entering the comment in the “Comment” field. You can also add or erase a comment in the comment column by clicking the “…” link.

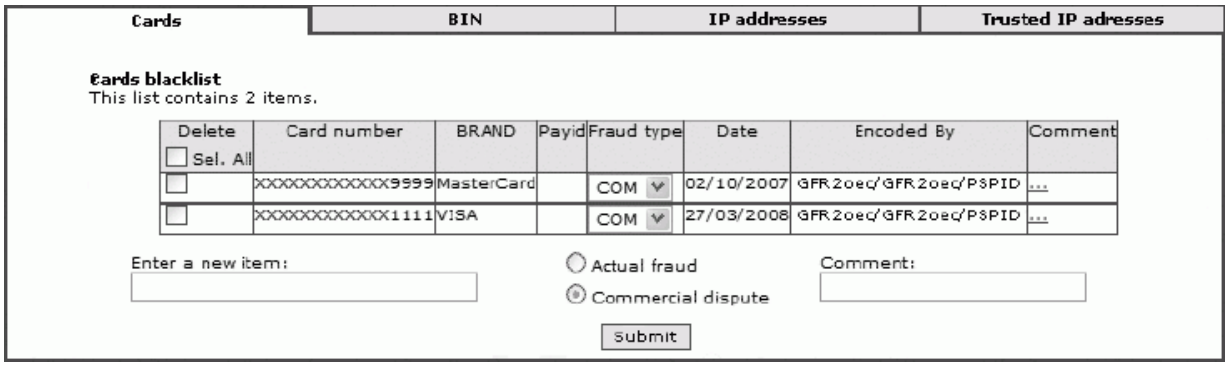
For each blacklist entry you can select the reason why you want to block the item: actual fraud or commercial dispute.

Note: Only select “actual fraud” as the type if the customer really has committed fraud, e.g. when a cardholder uses a card that does not belong to him.

4.1.1 Card blacklist

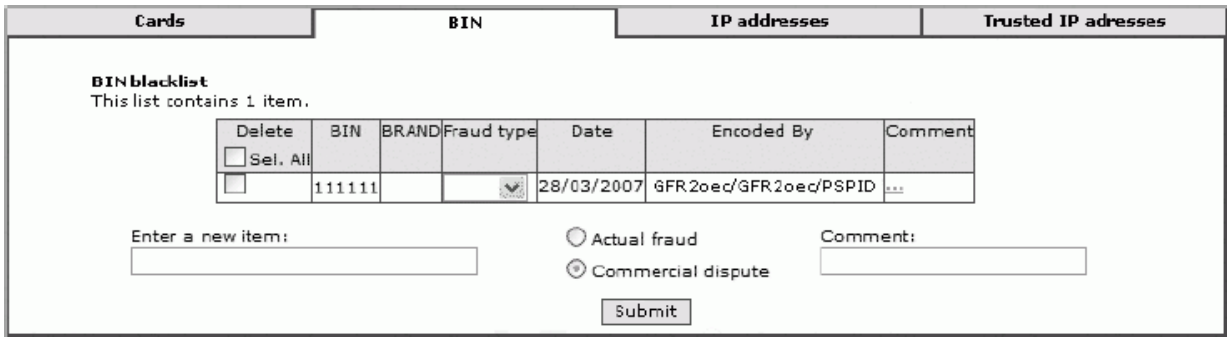
In your credit card blacklist, you must enter the full credit card number. You can always delete credit card numbers which have been entered on your list.

If you have activated the Direct Debits payment method in your account, the card blacklist will also double as account blacklist for entering account numbers



4.1.2 BIN blacklist

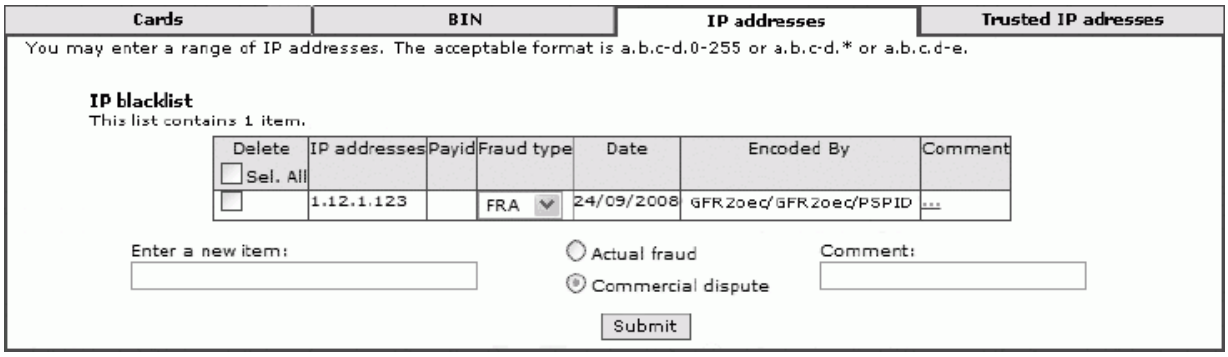
The BIN code is the first 6 digits of a credit card number. A BIN code is linked to a specific bank in a specific country. Consequently, you can enter all credit cards issued by bank X in country Y into your blacklist, simply by adding the BIN code. You can always delete BIN codes which have been entered on your list:



4.1.3 IP blacklist

In your IP addresses blacklist, you can not only enter a specific IP address, but also a range of IP addresses using the following formats: a.b.c-d.0-255 or a.b.c-d.* or a.b.c.d-e. You can always delete IP addresses which have been entered on your list.

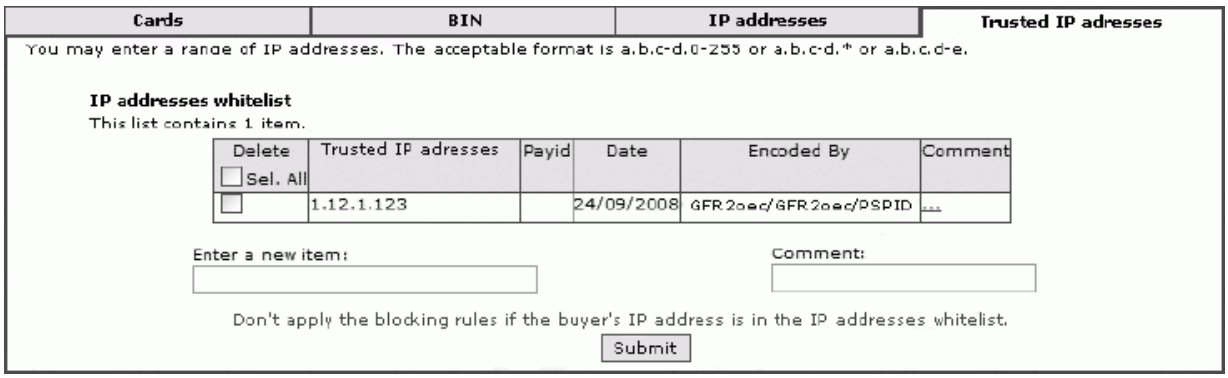
In order for our system to check the customer's IP address, merchants working via DirectLink need to send the IP address in the "REMOTE_ADDR" field.



4.1.4 IP whitelist

If, by blocking certain countries or IP address countries in the blocking rules, you have blocked a specific customer from whom you would like to accept orders, you can enter his IP address in the trusted IP address list. In this way you will allow transactions to be sent using this IP address, even though it may be from a country you have blocked. You can always delete IP addresses which have been entered into your list.

In order for our system to check the customer's IP address, merchants working via DirectLink need to send the IP address in the "REMOTE_ADDR" field.



5. Filters

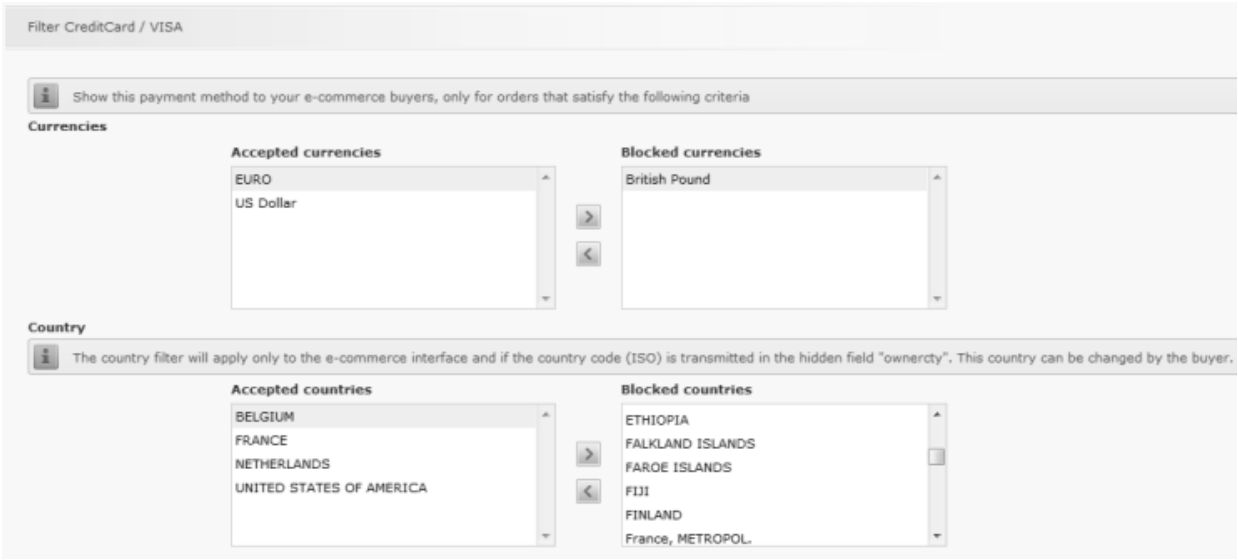
Filters are applicable before the customer has chosen his payment method. You can choose to hide specific payment methods from customers from a certain country or from customers paying in a certain currency on the orderstandard(UTF8).asp page (e-Commerce).

To configure a filter for a specific payment method, go to the payment method configuration page (“Payment methods” link in the menu) and click the “Edit filter” button next to the payment method.

If you do not set a filter, the payment method will be shown to all customers. If you wish to limit your payment method to certain currencies or countries, you can select them from the lists on the right-hand side of the screen.

Important: Before our system can apply the filters you set, you must either send your customer's country code in the hidden “OWNERCTY” field for each transaction, or enter “?” in the “OWNERCTY” field if you want our system to automatically detect your customer's country from his IP address. (for more information, go to e-Commerce)

The following screenshot shows the selection of EUR and USD as payment currencies that can be used for VISA transactions from Belgium, France, the Netherlands and the USA. If a customer has to pay an amount in GBP from the UK, he will not see VISA as a payment method in your payment methods list.



6. Feedback

6.1 Transaction view (in your PostFinance Account)

6.1.1 Advanced selection criteria

When you look up a transaction via the “View transactions” or “Financial history” link in your account menu, you will have "IP address" displayed as an extra option in the “Advanced selection criteria”. You can use the IP address field to look up all transactions from the same IP address or from IP addresses starting with the same digits.

6.1.2 Transaction list

When you display your transaction list via “View transactions” or “Financial History” in your back office, you will notice green spots and half spots in the list (if you have 3-D Secure activated for your account).

The full spot , where the thumb is up, represents a 3-D Secure transaction where the customer paid with a 3-D Secure registered credit card. With these transactions, your acquirer provides you with a conditional payment guarantee.

The half spot represents a 3-D Secure transaction where the customer has paid with a credit card that is not 3-D Secure registered. These transactions involve a certain level of conditional payment guarantee, based on the specific details in the 3-D Secure contract with your acquirer.

Transactions with no spot at all are transactions that have not been processed using 3-D Secure. The conditional payment guarantee will not apply to these transactions.

Transactions with an exclamation (warning) mark indicate transactions where the customer’s authentication failed. The conditional payment guarantee will not apply to transactions which you chose to proceed with (continue), where the authentication failed.

6.1.3 Transaction details

In the transaction details (Financial page), you will see additional information such as the card verification code result (if the CVC code has been entered by the customer), card country, IP address country and IP address.

The Dispute button above the table with the additional information will take you to a page where you can add certain transaction details to your blacklists with one click. This option allows you to add the card number used for a transaction to your blacklist without having to know the full card number, for instance.

You can also mark the transaction as a commercial dispute or fraud.

Note: Only select “actual fraud” as the type if the customer really has committed fraud with this card, for instance when a cardholder uses a card that does not belong to him.
Dispute:

6.1.4 Error codes

When a transaction has been retained by our system based on the rules you set in the Fraud Detection Module, you will find the reason in the error message for the transaction. With a few exceptions, all error codes related to Fraud detection begin with "300011", followed by two more digits.

Note: More information about statuses and error codes can be found online. Just log in to your PostFinance account and go to: Support > Integration & user manuals > User guides > List of the payment statuses and error codes.
The following non-exhaustive list contains examples of the most relevant ones:

3 / 30001100 Unauthorised customer's country
3 / 30001120 IP address on merchant's blacklist
3 / 30001130 BIN on merchant's blacklist
3 / 30001140 Card on merchant's card blacklist

6.2 Supplementary transaction parameters

In your post-sale requests, redirections with feedback, file downloads and DirectLink XML responses, supplementary transaction parameters relating to Scoring will be returned.

The list of supplementary parameters is set out below.

These fields will be empty if a format validation error occurred for the transaction details.

Format: AN= Alphanumeric / N=Numeric, maximum allowed amount of characters

Field	Description	Format
IPCTY	Originating country of IP address. Format: 2-character alphabetic ISO code. If this parameter is not available, “99” will be returned in the response. This IP check is based on externally provided IP listings, so there is a slight risk, as we rely on the accuracy of this list. The check gives positive results in 94% of all cases.	AN, 2

CCCTY	Originating country of credit card. This is only available for VISA, MasterCard and American Express. This value will be empty for all other brands/payment methods. Format: 2 character alphabetic ISO code. If this parameter is not available, “99” will be returned in the response. This credit card country check is based on externally provided listings, so there is a slight risk since we rely on the correctness of this list. The check gives positive results in 94% of all cases.	AN, 2
ECI	Electronic Commerce Indicator. The possible ECI values and their meaning are set out below: 1: Manually keyed 2: Recurring payments 3: Instalment payments 5: Cardholder identification successful 6: Merchant supports identification but not cardholder, conditional payment guarantee rules apply 7: E-commerce with SSL encryption 9: Recurring after first E-Commerce transaction 12: Merchant supports identification but not cardholder, conditional payment guarantee rules apply (idem 6) 91: Cardholder identification FAILED !!!! (Conditional payment guarantee (see here) may apply. Please check with your acquirer.) 92: Issuing bank authentication site temporarily unavailable, but transaction continued	N
CVCCHECK	Result of the card verification code check. Possible values: KO: The CVC has been sent but the acquirer has given a negative response to the CVC check, i.e. the CVC is wrong. OK: The CVC has been sent and the acquirer has given a positive response to the CVC check, i.e. the CVC is correct OR The acquirer sent an authorisation code, but did not return a specific result for the CVC check. NO: All other cases. For instance, no CVC transmitted, the acquirer has replied that a CVC check was not possible, the acquirer declined the authorisation but did not provide a specific result for the CVC check, etc.	AN, 2
AAVCHECK	Result of the automatic address verification. This verification is currently only available for American Express. Possible values: KO: The address has been sent but the acquirer has given a negative response for the address check, i.e. the address is wrong. OK: The address has been sent and the acquirer has returned a positive response for the address check, i.e. the address is correct OR The acquirer sent an authorization code but did not return a specific response for the address check. NO: All other cases. For instance, no address transmitted; the acquirer has replied that an address check was not possible; the acquirer declined the authorization but did not provide a specific result for the address check, etc.	AN, 2
VC	Virtual card. Possible values: ECB: For E Carte Bleue ICN: For Internet City Number NO: All other cases. For instance, the card is not a virtual card, the card is a type of virtual card not known to us, etc.	AN, 3

IP	Customer’s IP address, as detected by our system in a 3-tier integration, or sent to us by the merchant in a 2-tier integration.	AN, 15
More information about these fields can be found online. Just log in to your PostFinance account and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.		

7. CVC and AAV

7.1 CVC2

CVC2 is an authentication procedure established by credit card companies to assist in preventing fraudulent credit card use for Internet transactions. Depending on the brand, this code has a different name (CVC2 or Card Validation Code for MasterCard, CVV2 or Card Verification Value for VISA, CID or Card Identification Number for American Express). However, the code is generally referred to as the “CVC”. The functionality of the CVC2 is the same for all brands.

The verification code is uniquely linked to the card number, but is not part of the card number itself. Depending on the card brand, the verification code will be a 3 or 4-digit code on the front or rear of the card, an issue number, a start date or a date of birth. For MasterCard and VISA, for example, a 3-digit code is present on the back of the card in the signature strip, after the full customer account number or the last 4 digits of the customer account number.

It is strictly forbidden for merchants and PSPs to store customers’ CVC2 codes in a database. When the cardholder is not present in person, i.e. for "card not present" transactions, and he is asked to enter his CVC2 code together with his card number, this verification code helps ascertain that the customer placing the order has the actual card at hand and that the card account is legitimate.

7.2 AAV

AAV is an authentication procedure available in some markets to assist in preventing fraudulent credit card use for internet transactions. Depending on the brand, this authentication procedure has a different name (AVS or Address Verification Service/System for VISA/MasterCard; AAV or Automated Address Verification for American Express). However, the functionality of the AAV is the same for all brands.

The address check takes place when the acquirer requests the card issuer to compare the numeric components (house number and postcode / ZIP) of the customer’s (invoicing or delivery) address which the merchant sent us with those in the invoicing address given by the customer to the issuer when applying for the card.
American Express performs this check automatically when it receives address details with a transaction; for other brands, it depends on whether the acquirer performs the address check or not. Under all circumstances, we recommend that the customer’s address details should be sent together with the order details you send to our system.

Although a transaction will not be refused due to the outcome of the address check, the merchant may use this outcome to decide whether to deliver the goods or to ask the customer for further information before dispatching.

8. Fraud reporting tips

These are some tips you may be able to use in case of (suspicion of) fraud:

- The fraudulent use of a credit card has to be reported by the card holder himself to his issuing bank, i.e. the bank where he applied for his credit card.
- If you think one of your customers is committing fraud, you have to report this to your acquirer.
- If you want to report a fraudster to the police, you don’t need the credit card number. The information which is useful for the police is the IP address the customer used at the time of the transaction, with the date, time and time zone. If you can include the delivery address(es) with this information, the police have a greater chance of being able to trace the fraudster. Please note, however, that the IP address may be spoofed and the delivery address may only be the address of an intermediary who has to forward the goods to a foreign country; this would make it harder for the police to trace the fraudster.