Observatoire de la sécurité des moyens de paiement

www.observatoire-paiements.fr

FOR INFORMATION PURPOSE ONLY

Only the French version is binding

Initial publication on 10 June 2024
Last updated version dated from 18 April 2025

Fraud prevention measures on remote card payments outside *3-D Secure*

1. Context of the work

EU Directive No. 2015/2366 of 25 November 2015 on payment services, known as DSP2[1], transposed into French law into the Monetary and Financial Code[2], provides for the use of a strong customer authentication system for electronic payments, as well as for transactions carried out through a means of remote communication likely to involve a risk of fraud[3]. However, EU Delegated Regulation No. 2018/389 of 27 November 2017 (or RTS for standard technical standards) provides for exemptions[4] concerning, in particular, transactions carried out in favour of a trusted beneficiary, recurring transactions, low-value transactions or transactions with a low level of risk.

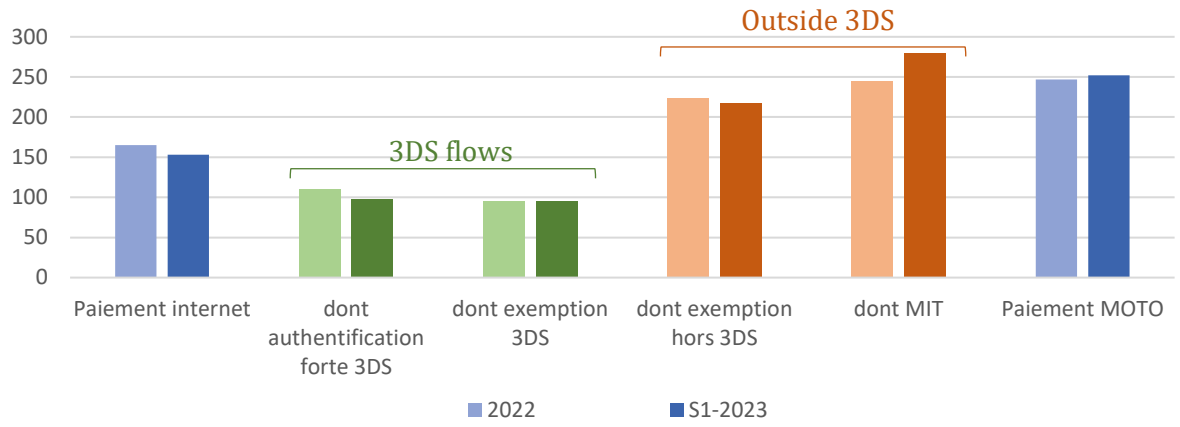
In France, the gradual implementation of strong customer authentication for remote payments made by credit card was carried out as part of the migration plan adopted by the Observatory[5].

This implementation was made possible by the deployment of the second version of the 3-D Secure protocol, intended for the management of exchanges between the merchant, the cardholder and their payment service providers (PSP), for the purpose of authentication of payments over the Internet. Version 2.0 of the protocol allows the management of strong remote payment authentication using the various solutions currently offered to cardholders by PSP issuers, and which also supports requests for exemption from strong customer authentication.

The implementation of strong customer authentication has reduced the fraud rate on remote payments made via 3-D Secure. The fraud rate now appears to be under control on all these payments, including those with a strong customer authentication exemption (Figure 1).

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market
[2] Articles L. 133-1 et seq.
[3] Article L. 133-4, I of the Monetary and Financial Code
[4] Articles 11 to 18 of EU Regulation No 2018/389
[5] Chapter 1 of the 2018 annual report of the Observatory

Figure No. 1: card fraud rate *(in € of fraud / € 100,000 of payments)*



Conversely, the fraud rate remains structurally higher today on payments made remotely outside 3-D Secure, including MIT-type (Merchant Initiated Transaction) payments, as well as MOTO (for Mail Order – Telephone Order) payments.

By nature, these payments, which do not give rise to any authentication at the time of their issuance, are much more exposed to fraud than payments transiting through the 3-D Secure protocol:

- such payments may be initiated by any person who has been able to obtain the data recorded on the bank card (number and expiry date for MOTO payments, and visual cryptogram in addition for MIT payments), without this person even needing to be in possession of the card or to be able to have access to the strong customer authentication device for remote payments;
- in particular, a merchant may transmit payments to his PSP that do not correspond in reality to any product or service delivered to the cardholder, for example, by reusing payment card data previously used in legitimate transactions;
- in terms of MOTO payments in particular, these are based on the communication by the payer of the number of their credit card and its expiry date through an insecure channel (telephone conversation, email, mailing, fax ...); then on the handling by an operator who ensures their entry on the merchant's payment terminal. This situation promotes internal or external fraud by misappropriation of payment data.

While the technical standards in force theoretically include the possibility of implementing a MOTO payment authentication solution, this possibility is not used in practice and no uniform solution for the authentication of these payments has been identified to this date.

In addition, MOTO payments and non- 3-D Secure internet payments are sometimes diverted from their original purpose to allow a merchant to accept customer-initiated internet payments (CIT), thus bypassing the strong customer authentication obligation imposed by the DSP2.

These findings lead the Observatory to adopt recommendations that aim to prevent fraud on remote payments made outside 3-D Secure.

These recommendations, published on 10 June 2024 in their initial version, have been the subject of adjustments incorporated in the versions published on 13 and 27 August 2024. The current version also takes into account the contributions of the 2025 roadmap, validated at the plenary meeting of the Observatory on 19 December 2024.

2. Scope of recommendations

These recommendations apply to all remote payments without strong customer authentication made outside 3-D Secure, namely:

- on the one hand, MOTO payments ;
- on the other hand, non-3-D Secure internet payments, including MIT payments (for which only the strong customer authentication performed during the validation of the mandate uses the 3-D Secure channel), as well as CIT payments requesting the benefit of an exemption without transiting through the 3-D Secure protocol (then referred to as DTA payment for direct to authorisation).

As an exception, these recommendations do not apply:

- to non-3-D Secure internet payments recognized as strongly authenticated by the issuing PSP, such as payments made using a mobile wallet solution, for which the merchant, PSP, scheme or mobile solution provider provide a strong customer authentication solution in compliance with PSD2;
- electronic payments initiated by legal entities by means of dedicated payment procedures or protocols that are only made available to payers who are not consumers, when the competent authorities have acquired the certainty that said procedures and protocols guarantee security levels at least equivalent to those provided for by the DSP2[6];
- payments for which the acquiring PSP is located outside the European Economic Area, with a specific exception for acquirers located in the United Kingdom and Switzerland:
    - [New] From May, 12th 2025, those recommendations also apply to payments for which the acquiring PSP and the beneficiary merchant are located in the United Kingdom or Switzerland, because those countries are also used to have recourse to *3-D Secure* for internet card-based payments.

These recommendations are intended to be implemented by merchants who accept such payments, by their technical acceptance providers, by the various card schemes as well as by all PSPs, whether they are issuers and/or buyers.

3. Recommendations for remote payments outside 3-D Secure

3.1 Use of MOTO payments and non-3-D Secure internet payments only when the use of another payment method is not possible

The high rate of fraud on these payments requires limiting MOTO payments, as well as non- 3-D Secure internet payments (other than those recognized as authenticated by the issuing PSP, for example when using a wallet) to the only use cases for which these payment methods are intended.

In particular, internet payments that may benefit from an exemption from strong customer authentication are intended to be presented via 3-D Secure. Indeed, this protocol allows the management of exemption requests, and the strong customer authentication request of the client when the exemption request is rejected via soft decline.

[6] Such payments shall be exempt from the strong customer authentication obligation pursuant to Article 17 of EU Regulation No 2018/389.

In any case, the issuing PSP is in charge to enforce a strong customer authentication, even if an exemption request has been sent to it. The *Data Share Only* feature included in *3-D Secure* protocol is consequently not compliant with these recommendations. In order to promote frictionless, when a payment is eligible to several exemption categories (for example, low value payment exemption and Transaction Risk Analysis exemption), the merchant and the acquiring PSP are invited to request the exemption which is better supported by the issuing PSPs, for example the TRA exemption inside the 2.2 version, today mostly deployed, of *3-D Secure* protocol.

Recommendation No. 1: limiting MOTO and MIT payments to use cases only or using another payment method is not possible

Merchants ensure:

- **to accept payments by MOTO card only for contracts subscribed remotely by a channel (phone, mail ...) other than the Internet. They shall ensure the use of a proximity payment or a secure payment by internet whenever the nature of a contract and the terms of its subscription as well as the delivery of the goods or services ordered are compatible with such a payment (for example, point-of-sale payment at the time of delivery, made directly by the merchant, of goods ordered by telephone);**
- **to accept payments over the internet only via the secure 3-D Secure channel, except in cases where the payment is recognized as strongly authenticated by the issuer (for example when using a wallet integrating strong customer authentication) and use cases that do not allow the use of 3-D Secure, such as MIT payments.**

In particular, merchants should never resort to non-3-D Secure internet payments and MOTO payments when the payment is made via the internet and was initiated by the customer (CIT).

Technical acceptance providers and acquiring payment service providers shall ensure compliance with this recommendation by merchants with whom they have entered into an acceptance contract.

3.2 Valid chaining of MIT payments

The use of the 3-D Secure protocol for all customer-initiated internet payments (CIT) should lead to the reservation of non-3-D Secure internet payments other than those recognized as authenticated by the issuing PSP (for example when using a wallet integrating a strong customer authentication solution) to payments initiated by the merchant (MIT).

Each MIT payment must be associated with a valid chaining reference allowing the card issuer to ensure the consent of its cardholder to the payment presented or, when processing a dispute formulated by the cardholder, to reconcile the payment and the mandate previously validated by the means of a strong customer authentication.

If the absence of chaining can be detected upon acceptance of the payment by the issuing PSP, the analysis of the validity of the chaining (i.e. ensuring that the chaining presented corresponds to prior authentication) cannot be carried out in real time by the latter. As a result, invalid chaining, i.e. not corresponding to a payment mandate duly validated by the cardholder by the means of a strong customer authentication, can only be detected by making an a posteriori reconciliation that the issuing PSPs are invited to gradually implement.

Recommendation No. 2: valid MIT chaining

When issuing an MIT payment, merchants communicate to their PSP the chaining reference resulting from the validation by strong customer authentication of the payment mandate authorizing the payment.

Issuer PSPs are invited:

- **to gradually implement a reconciliation mechanism between the chaining of MIT payments and payment mandates validated by strong customer authentication;**
- **to notify merchants and technical acceptance providers of the anomalies identified in the chains presented in the MIT transactions they issue so that they can implement an action plan to remedy them;**
- **in the absence of remediation, to apply the velocity limit defined by Recommendation No. 3 to MIT payments presented by merchants and/or technical acceptance providers concerned by the use of invalid chaining references.**

3.3 Limitation of the velocity of MOTO payments and internet payments outside 3-D Secure and specific measures applicable to priority merchants to fight fraud

The prevention of fraud on MOTO payments and on non- 3-D Secure Internet payments (outside of cases where the operation is considered by the issuing PSP as strongly authenticated) requires limiting velocity, i.e. the cumulative amount of purchases made with the same card from the same merchant during a period of 24 hours (sliding).

Velocity = cumulative amount of purchases / card / merchant / 24 hours

Velocity is measured separately for MOTO payments on the one hand, and for non-3-D Secure internet payments on the other.

The Observatory invites the issuing PSPs to reject any operation leading to the exceeding of this limit, by soft decline when the characteristics of the operation allow this mode of rejection.

This velocity limit does not concern:

- the sectors of activity for which the use of the payment method (MOTO and/or MIT) appears justified and for which the fraud rate is controlled. These sectors are included in the "exemption list" defined in Appendix 2;
- MIT payments associated with a technically valid chaining reference and for which the merchant and the technical acceptance provider have not been identified as issuing payments associated with chaining references presenting anomalies.

In addition, individual derogations may be granted, depending on the rate of fraud observed for each merchant, and according the procedure defined in Appendix 3[7].

Conversely, the exemption may be waived, upon decision of an issuing PSP and for the duration of its choice, for a merchant whose MCC benefits from an exemption but who makes inappropriate use of MOTO payments or internet payments outside 3-D Secure, or whose fraud rate on these payments appears insufficiently controlled with regard to the criteria defined by the issuing PSP.

Recommendation No. 3: velocity limit and implementation of a soft decline mechanism

[7] A merchant is identified, when issuing a card payment, by the value entered in the *Merchant ID field* included in the data of this payment.

The PSP issuers reject, by soft decline where possible, MOTO payments and non-3-D Secure Internet payments recognized as not strongly authenticated by the issuer, as soon as the amount of the payment would lead to the exceeding of the velocity limit defined by this recommendation.

The velocity limit is assessed over a period of 24 sliding hours, and is measured separately:

- **on the one hand, for MOTO payments;**
- **on the other hand, for internet payments outside 3-D Secure. For this payment category, the velocity measurement does not take into account either CIT payments authenticated by the issuer (for instance by mobile wallet), or MIT payments associated with a valid chaining reference.**

For MOTO payments, the velocity limit is set at 500 euros since 10 June 2024.

For internet payments outside 3-D Secure, the velocity limit is set at 100 euros since 14 October 2024.

This limit will be lowered to:

- **50 euros, starting from 10 February 2025 onwards;**
- **30 euros from 10 March 2025 onwards;**
- **[Updated] 10 euros from 10 April 2025 onwards**
- **[Updated] 1.01 euro from 12 May onwards: from this date, internet payments outside 3-D Secure, which are strictly higher than 1 euro, will no longer be admitted. This rule does (i) neither apply to CITs recognized by the issuer as strongly authenticated, (ii) nor to MITs associated to a valid chaining reference, (iii) nor to 0 euro information requests, and (iii) nor to 0 euro pre-authorizations.**
- **[New] Merchants are invited to check the qualification of their authorization requests ≤ 1 euro, to make a difference between authorization requests and other use cases (card verification, balance inquiry, preauthorization etc.), because this limit could be lowered down to 0.01 euro from 1 January 2026.**

The following are excluded from the application of this recommendation:

- **payments accepted by merchants who benefit from an exemption (for the type of payment concerned) granted under the conditions defined in Appendix 2 or 3;**
- **MIT payments that are associated with a valid chaining reference;**
- **MOTO payments that have been the subject of strong cardholder authentication.**

The implementation of velocity limits will be supervised by a steering committee under the aegis of the Observatory's "strong customer authentication" working group.

This steering committee will be responsible for:

- verifying that all legitimate use cases of MOTO payments and non- 3-D Secure internet payments have been taken into account and that the implementation of the velocity limit does not lead to the rejection of legitimate transactions;

– if necessary, adjusting the terms of implementation of this recommendation and in particular to propose changes to the list of activity sectors excluded from its application to differ the application dates for the 2nd and 3rd threshold.

By derogation to recommendation No.3, merchants, benefiting from a sectoral exemption for MOTO payments but accepting an important volume of MOTO payments and whose exposure to fraud for these payments is frequently higher than the average of all merchants, will be qualified as priority and subject to a velocity limit, if no action plan is presented to the Banque de France. These terms aim at incentivising the implementation of a dialogue between the merchants concerned and the issuing PSPs.

The identification of priority merchants is done by the issuing PSPs in association with the Banque de France, and in accordance with criteria set out in Appendix 4.

This approach is in line with the prospect of a progressive replacement of sectoral exemptions by individual derogations, granted according to the terms and criteria defined in Appendix 3.

Recommendation No. 3a: specific measures applicable to merchants identified as priority merchants for fraud reduction on MOTO payments

Merchants benefiting from a sectoral exemption for MOTO payments but accepting an important volume of MOTO payments and whose exposure to fraud for these payments is frequently higher than the average, in accordance with criteria set out in Appendix 4, are identified as priority merchants and subject to specific measures.

Merchants identified as priority merchants, and who have been notified by their acquiring PSPs as well as trough card schemes, must present an action plan to the Banque de France.

In the absence of such a plan, which must be validated by the Banque de France one month after the notification of the merchant as priority, the latter will be subject to a velocity limit for its MOTO payments, which will be gradually decreased down to 500 euros. The calendar would be communicated by the Banque de France to the merchant.

Likewise, merchants accepting an important volume of MIT payments and whose exposure to fraud for these payments is frequently higher than the average of all merchants, will be qualified as priority and subject to specific measures implemented by the issuing PSPs (rejection of 0-euro information requests, rejection of MIT transactions with an high-risk fraud score….). This approach aims first at preventing manifestly inadequate use of MITs with regard to the business model (e.g. Internet payments made in the presence of the cardholder), but also at incentivising the setup of a dialogue between the priority merchant and the issuing PSPs. The identification of those priority merchants is done by the issuing PSPs in association with the Banque de France, and in accordance with criteria set out in Appendix 4.

[New] Recommendation No. 3b: specific measures applicable to merchants identified as priority merchants for fraud reduction on MIT payments

Merchants accepting an important volume of MIT payments and whose exposure to fraud for these payments is frequently higher than the average, in accordance with criteria set out in Appendix 4, are identified as priority merchants and subject to specific measures.

Merchants identified as priority merchants, and who have been notified by their acquiring PSPs as well as trough card schemes, must present an action plan to the Banque de France.

In the absence of such a plan, which must be validated by the Banque de France one month after the notification of the merchant as priority, the latter will be subject to specific measures, which are proposed by the issuing PSPs and validated by the Banque de France.

3.4 Security of payments data transmitted by the payer during a MOTO payment

Merchants that accept MOTO payments must pay particular attention to the security of the payment data they handle, in order to prevent their misuse.

With regard to payments such as Telephone Order, the use of a voice server makes it possible to avoid the manipulation of data by an operator: the paying customer enters his payment data directly on the keyboard of his phone with voice frequencies (whether a landline, a mobile phone or a smartphone) and the server automatically transmits this data to the payment terminal, to allow the acceptance of the payment.

Depending on the use case, the customer may either be in contact only with the voice server (for example for the payment of an invoice: the customer will then enter the invoice reference before entering his payment data), or be in contact with an operator to whom he indicates the characteristics of the goods or services he wishes to order, before being in contact with the voice server at the time of making the payment.

Recommendation No. 4: securing payment data

Merchants who accept MOTO payments ensure the security of payment data communicated by customers. Merchants who accept payments by telephone (Telephone Order) ensure that, when possible, customers communicate their payment data to a controller (for example by typing on the phone keyboard or using a voice recognition mechanism) rather than to an operator.

Acquiring payment services providers shall ensure compliance with this recommendation by merchants with whom they have entered into an acceptance contract.

3.5 Experimentation with authentication of MOTO payments

The implementation of an authentication mechanism, even simple (a single authentication factor), for MOTO payments would improve the level of security since these payments are not currently the subject of any authentication.

In some cases, this authentication could rely on existing devices, such as mobile application authentication of payments made by phone, for cardholders enrolled in the strong mobile application authentication solution offered by their PSP, or by entering a single-use password received by SMS.

Some strong customer authentication solutions designed for internet payments appear incompatible with telephone payments, which do not allow the entry of an alphanumeric password. The particular typology of customers who use telephone payments (for example, customers who do not have internet access and/or a mobile phone line) should also be taken into consideration.

Recommendation No. 5: experimentation with authentication of MOTO payments

Merchants and payment service providers (PSPs) are encouraged to offer authentication solutions for MOTO -type payments tailored to each payment channel and the relevant customer typology.

The Observatory also calls on all actors of the payment chain (payment cards schemes, payment services provides, technical providers, electronic payment standard prescribers…) to work towards the development of a strong customer authentication solution for telephone payments (TO) by the fourth quarter of 2025.

APPENDIX 1: Glossary

PSP: payment service provider.

Acquiring PSP: PSP of the beneficiary, i.e. the merchant who accepts payments by card.

Issuer PSP: PSP of the payer, i.e. PSP that issues the card.

CIT: Customer Initiated Transaction, transaction initiated by the customer. This category covers the majority of card payments made directly by the cardholder on e-commerce sites.

MIT: Merchant Initiated Transaction, transaction initiated by the merchant. This category corresponds in particular to payments whose exact amount is not known in advance, recurring payments (subscriptions) or split payments (payment in several times), according to an operation comparable to that of a SEPA debit: the customer subscribes to a mandate, validated by strong customer authentication, by which he authorizes the merchant to initiate one or more subsequent payments under predefined conditions (unit amount, ceiling, frequency, etc.).

MOTO: Mail Order – Telephone Order, payments for which the cardholder communicates to the merchant by telephone, postal mail, email, fax ... the number of his card and the expiration date, data that the merchant then enters on his electronic payment terminal. This payment method is intended for the payment of purchases made by telephone (for example: travel or hotel reservation) or by sending a purchase order on paper.

Chaining: cryptographic authentication reference, in the form of an alphanumeric string, communicated by the issuing PSP following the strong authentication of the client during the validation of the MIT mandate. This reference allows PSPs to identify the highly authenticated mandate under which one or more payments are then issued by the merchant.

Soft decline: mechanism by which the PSP acquirer or issuer rejects a card payment with an exemption request while allowing the merchant (or its technical acceptance provider) to resubmit the payment request via the 3-D Secure protocol (so-called retry operation). The rejection is transparent for the cardholder who does not have to re-enter his payment data; however, the cardholder will have to validate the payment by strong authentication.

Velocity: cumulative amount of payments made using the same card with the same merchant during the same sliding reference period (24 hours).

APPENDIX 2: Procedure for the exemptions to the velocity limit mechanism by activity sector and updated list of the sectoral exemptions in force

A list of activities exempted from the velocity limit is defined, for each category of payments (MOTO payments and Internet payments outside 3-D Secure), according to the MCC (Merchant Category Code) assigned to the merchants from this activity sector.

The following list may be adjusted, depending on the fraud rates and use cases observed, by the Observatory's « strong customer authentication » working group. The current list of exemptions in force is available on the Observatory's website.

Reasons for requesting a sector exemption

In accordance with the present recommendations, the aim is to identify the activity sectors for which the use of the payment method in question (MOTO and/or internet payment outside 3-D Secure) appears justified, and for which the fraud rate is under control. A sector that suffers a significant deterioration in its acceptance rate following implementation of the plan, while still having a limited fraud rate, may request an exemption.

Procedure to be followed

For an exemption to be granted to an activity sector, a request must be sent to the Observatory secretariat (2323-OSMP-ut@banque-france.fr), stating the reason and the elements listed below. The request may be submitted by one of the sector representatives, a merchant representative, a payment card scheme or an acquiring PSP. The Observatory secretariat may also directly propose an exemption for an activity sector.

List of elements to provide

- Description of the activity
- Technical data: MCC
- Payments category for which the exemption request is formulated: MOTO payments or internet payments outside 3-D Secure
- Volume of operations (in number and in amount) for the MCC and the payments category concerned
- Number and amount of refusals linked to the implementation of the plan and the current phase (thresholds of €500, €250 or 100 euros).

Eligibility criteria

In order to become eligible for an exemption, the MCC must meet the following criteria (cumulatively):

1. Criterion linked to fraud

The fraud rate observed for the MCC on internet payments outside 3-D Secure or MOTO is less than 0.13% in amount, over an ideally annual period (and in any case at least six months to avoid seasonal effects).

2. Customer and merchant inconvenience criterion

The rate of refusals in number or amount on MCC transactions linked to the implementation of the recommendations must be greater than 10%. This rate is calculated from the date on which implementation of the recommendations begins (7 June 2024) or from one of its intermediate milestones linked to the successive lowering of the velocity limit.

After gathering the analysis of payment card schemes and issuing PSPs, the steering committee under the aegis of the Observatory's Strong Customer Authentication WG grants or refuses the exemption request, and informs the applicant of the decision. The updated list of exemptions is published on the Observatory's website.

List of MCC currently benefiting from an exemption

Internet payments outside 3-D Secure

None

MOTO Payments

1771 CONCRETE
2741 PRESS
3000 to 3299 AIRLINE COMPANIES *(MCCs attributed individually)*
3350 to 3449 CAR RENTAL COMPANIES *(MCCs attributed individually)*
3500 to 3999 HOTEL COMPANIES *(MCCs attributed individually)*
4011 RAILROADS
4112 PASSENGER RAILWAYS
4411 MARITIME TRANSPORT
4511 AIR TRANSPORT
4722 TRAVEL AGENCY
4814 TELECOMMUNICATION SERVICES
4900 SERVICES ELECTRIC, GAS, WATER, SANITARY
5965 COMBINATION CATALOGUE AND RETAIL MERCHANTS
6010 CREDIT DISTRIBUTION
6012 FINANCIAL INSTITUTIONS
6300 INSURANCE
6513 LEASE LODGING
7011 MOTELS HOTELS ACCOMMODATION
7032 COLONIES AND HOLIDAY CAMPS OR SPORTS ACTIVITIES
7033 OTHER TOURIST ACCOMMODATION
7322 DEBT COLLECTION AGENCIES
7512 CAR RENTAL AND LEASE
8111 LEGAL SERVICES AND LAWYERS
8220 HIGHER EDUCATION
8398 SOCIAL AND CHARITABLE WORKS
9405 PURCHASES BETWEEN AGENCIES OF THE SAME ADMINISTRATION

APPENDIX 3: Merchant derogation procedure to the velocity limit

In accordance with the present recommendations, individual derogations can be granted, depending on the fraud rate observed for each merchant. The present appendix details the derogation process for a merchant, for internet payments outside 3-D Secure or MOTO Payments.

Reason for requesting a derogation for a merchant

Merchants who experience a significant deterioration in their acceptance rate following implementation of the recommendation may request a waiver from the Observatory secretariat (2323-OSMP-UT@banque-france.fr), either directly or via their acquiring PSP or any other member of the steering committee. Merchants are strongly advised to contact their technical acceptance service provider and/or their acquiring PSP to request such a waiver.

Procedure to follow

In order for a merchant to benefit from a derogation, the application must specify the reason and duration of the derogation, and include a commitment by the merchant to ensure the security and compliance of its payment transactions. The derogation, including its period of validity, must be validated by the Banque de France, after obtaining the opinions of representatives of issuing PSPs and payment card schemes who are members of the steering committee.

List of elements to provide

- Description of the merchant's activity
- Technical data : acquired BIN/ICA, MCC, Merchant ID/Card acceptor ID, Card acceptor name
- Payments category for which the request is formulated : MOTO payments or internet payments outside 3-D Secure
- Volume of operations in number and in amount linked to the merchant activity for the payments category concerned
- Actions already implemented for the prevention and detection of fraud
- Planned actions to reach compliance and fight against fraud
- Derogation duration requested

Eligibility criteria

1. Criterion linked to fraud or inconvenience

To benefit from an exemption, the merchant must justify that it is experiencing one of the following situations:

- The fraud rate observed for the merchant on internet payments outside 3-D Secure or MOTO is less than 0.13% in amount, over an ideally annual period (and in any case at least six months to avoid seasonal effects).
- **Or** the refusal rate in number or amount on merchant transactions linked to the implementation of the recommendations must be greater than 20%. This rate is calculated from the date on which implementation of the recommendations begins (7 June 2024), or from one of its intermediate milestones linked to the successive lowering of the velocity limit.

2. Criteria related to anti-fraud actions

In addition, the granting of the derogation is conditioned:

- To the actions already implemented by the merchant related to fraud prevention and detection ;
- To the actions planned by the merchant to reach compliance and fight against fraud.

After gathering the analysis of payment card schemes and issuing PSPs represented at the steering committee, the Banque de France grants or refuses the derogation request, and informs the applicant of the decision. The list of derogations granted is not public.

[New]

APPENDIX 4: Identification criteria of priority merchants targeted by recommendations No 3a and 3b

The total amount of fraud for a specific merchant and its associated fraud rate are calculated on a monthly basis for each type of transaction (MOTO on the one side, MIT on the other side) but for the full set of acquiring PSPs used by this merchant (in a case of a merchant, who has recourse to many acquiring PSPs).

MIT payments

- The merchant is on « incident » for one issuing PSP if:
  - Either its total amount of fraud is higher than 5,000 euros / month and its fraud rate in value is higher than 0.13%;
  - Or its total amount of fraud is higher than 10,000 euros / month and its fraud rate in value is higher than 0.05%;
- The merchant is identified as « priority » if it is on « incident » during 4 of the last 6 months for at least 3 out of the 7 major French issuing PSPs;
- The merchant is no longer identified as « priority » if it is not flagged as on « incident » during 3 consecutive months for at least 3 out of the 7 major French issuing PSPs.

These two subsets of criteria make it possible to target, on the one hand, merchants who do sufficiently control their fraud rate (first subset) and, on the other hand, merchants, who present a significant amount of fraud in value despite a low fraud rate (second subset).

MOTO payments

- The merchant is on « incident » for one issuing PSP if its total amount of fraud is higher than 5,000 euros and its fraud rate in value is higher than 0.13%.
- The merchant is identified as « priority » if it is on « incident » during 4 of the last 6 months for at least 3 out of the 7 major French issuing PSPs;
- The merchant is no longer identified as « priority » if it is not flagged as on « incident » during 3 consecutive months for at least 3 out of the 7 major French issuing PSPs.