



Gestion des risques avancée

Manuel d'utilisation du Back Office

Version du document 2.1

Sommaire

1. HISTORIQUE DU DOCUMENT.....	4
2. PRÉSENTATION DE LA FONCTIONNALITÉ.....	5
2.1. Prérequis.....	5
2.2. Comprendre la cinématique des contrôles.....	6
3. PRINCIPE DE FONCTIONNEMENT.....	7
3.1. Gestion des risques et authentification 3D Secure.....	7
3.2. Les critères.....	8
3.3. Les actions.....	9
4. CONFIGURER LA GESTION DES RISQUES AVANCÉE.....	11
4.1. Onglet Configuration.....	12
4.2. Onglet Résultat 3D Secure.....	13
4.2.1. Paiement 3D Secure avec un porteur dont l'authentification ne peut pas être vérifiée.....	14
4.2.2. Carte non enrôlée au programme 3D Secure.....	14
4.2.3. Paiement 3D Secure avec une carte dont l'enrôlement ne peut pas être vérifié.....	15
4.2.4. Transfert de responsabilité.....	15
4.3. Onglet Montant.....	16
4.3.1. Contrôle sur le montant.....	16
4.3.2. Contrôle sur le montant minimum.....	17
4.3.3. Contrôle sur le montant maximum.....	18
4.3.4. Contrôle du montant cumulé pour un moyen de paiement sur une semaine.....	19
4.4. Onglet Moyen de paiement.....	20
4.4.1. Contrôle des cartes commerciales.....	20
4.4.2. Contrôle des cartes commerciales suivant leur provenance.....	21
4.4.3. Contrôle des cartes prépayées.....	22
4.4.4. Contrôle des cartes à autorisation systématique.....	23
4.4.5. Contrôle des e-Carte-Bleue.....	24
4.4.6. Contrôle des cartes personnelles de crédit.....	25
4.4.7. Contrôle des cartes personnelles de débit.....	26
4.5. Onglet Panier.....	27
4.5.1. Contrôle sur le nombre de produits du panier.....	27
4.5.2. Contrôle des produits du panier.....	28
4.6. Onglet Pays.....	29
4.6.1. Contrôle du pays de l'acheteur (adresse de facturation).....	29
4.6.2. Contrôle du pays de livraison.....	30
4.6.3. Contrôle de la variété des pays.....	31
4.6.4. Contrôle sur des produits carte provenant de certains pays.....	32
4.6.5. Contrôle des pays pour les paiements SDD.....	33
4.7. Onglet Fréquence d'utilisation.....	34
4.7.1. Fréquence d'utilisation d'une adresse e-mail sur une semaine.....	34
4.7.2. Fréquence d'utilisation d'une adresse IP sur une semaine.....	35
4.7.3. Fréquence d'utilisation d'un moyen de paiement sur une semaine.....	35
4.8. Onglet Media.....	36
4.9. Onglet Résultat SafeKey.....	37
4.9.1. Carte non enrôlée au programme SafeKey.....	37
4.9.2. Paiement avec une carte dont l'enrôlement au programme SafeKey ne peut pas être vérifié.....	38
5. CRÉER DES RÈGLES DE NOTIFICATIONS SPÉCIFIQUES À LA GESTION DU RISQUE.....	39
6. TRANSMETTRE LES DONNÉES UTILES À LA GESTION DES RISQUES AVANCÉE.....	41
6.1. Transmettre les données de la commande.....	41
6.2. Transmettre les données de l'acheteur.....	43

6.3. Transmettre les données de livraison.....	45
7. CONSULTER LE DÉTAIL D'UNE TRANSACTION DANS LE BACK OFFICE MARCHAND.....	47
8. VALIDER MANUELLEMENT UNE TRANSACTION.....	49
9. RESTITUTION DU RÉSULTAT DU MODULE DE GESTION DES RISQUES AVANCÉE DANS L'IPN.....	50
10. OBTENIR DE L'AIDE.....	51

1. HISTORIQUE DU DOCUMENT

Version	Auteur	Date	Commentaire
2.1	La Banque Postale	10/01/2024	Mise à jour des chapitres : <ul style="list-style-type: none">• Onglet Configuration• Onglet Résultat 3D Secure
2.0.	La Banque Postale	17/08/2022	<ul style="list-style-type: none">• Mise à jour de la description des valeurs du champ vads_risk_assessment_result dans le chapitre <i>Restitution du résultat du module de gestion des risques avancée dans l'IPN.</i>

Ce document et son contenu sont strictement confidentiels. Il n'est pas contractuel.
Toute reproduction et/ou distribution de tout ou partie de ce document ou de son contenu à une entité tierce sont strictement interdites ou sujettes à une autorisation écrite préalable de La Banque Postale. Tous droits réservés.

2. PRÉSENTATION DE LA FONCTIONNALITÉ

La plateforme de paiement Scellius est une solution de paiement certifiée PCI-DSS hautement sécurisée. Toute tentative de paiement s'accompagne systématiquement d'une demande d'autorisation auprès de la banque du porteur. Dans le cas où le marchand est enrôlé auprès de CB, Visa, Mastercard, American Express ou Diners Club le processus de paiement comporte aussi une authentification du porteur.

Cependant, la vente à distance peut présenter des risques d'impayés préjudiciables à votre activité.

De manière à fournir un niveau de sécurité supplémentaire au marchand, la plateforme de paiement met à disposition la fonction **Gestion des risques avancée**.

Grâce à cette fonctionnalité, il est possible de :

- minimiser les risques d'impayés en refusant des transactions jugées frauduleuses ;
- ajouter des contrôles en cas de suspicion de fraude.

La fonction **Gestion des risques avancée** est un moyen flexible et personnalisable pour vous aider dans la lutte contre les fraudes. Des filtres pertinents sont mis à disposition pour définir des actions préventives en fonction du niveau de risque et des spécificités de votre activité sans pour autant pénaliser vos ventes. En effet, la gestion des risques avancée peut être configurée en tenant compte des risques connus ou des problèmes de fraude vécus par le passé. A vous d'adapter vos règles en fonction du profil de vos acheteurs et des transactions réalisées.

2.1. Prérequis

Le marchand doit souscrire à la fonction **Gestion des risques avancée** auprès de sa plateforme de paiement.

Une fois activée le marchand peut :

- accéder à la configuration depuis le Back Office,
- bénéficier du service offert par le module pour appliquer la protection (personnalisée) lors du processus du paiement.

Pour plus d'informations, contactez le Service Assistance Monétique Commerçants.

2.2. Comprendre la cinématique des contrôles

La fonction **Gestion des risques avancée** peut-être appelée plusieurs fois lors de la création d'un paiement :

- Au maximum trois (3) fois :
 - après la validation des données d'entrée ;
 - après l'authentification du porteur ;
 - après l'autorisation.

A chaque appel, le service retourne potentiellement une ou plusieurs actions qui impactent le processus de paiement. Tous les paiements (paiement unitaire, paiement différé, paiement en plusieurs fois, paiement multiscarte, etc.) sont concernés par les contrôles de la **Gestion des risques avancée**.



En cas d'indisponibilité, de configuration incorrecte, ou de dysfonctionnement, le paiement s'effectue comme si le marchand ne possédait pas la fonction de gestion des risques avancée.

3. PRINCIPE DE FONCTIONNEMENT

La plateforme propose un ensemble de profils de gestion de risque. Chaque profil est constitué d'une ou de plusieurs règles. Chaque règle et chaque profil peuvent être activés ou désactivés.

Une règle est constituée de :

- un ou plusieurs critères à valider ;
- une ou plusieurs actions qui seront déclenchées si tous les critères de la règle sont validés.

Exemples :

- Une règle simple avec un seul critère et une seule action : si le montant cumulé sur une semaine est supérieur à 500 EUR, refuser le paiement.
- Une règle plus complexe avec deux critères et une action : si le pays de l'acheteur est différent du pays de la boutique du marchand et que le montant est supérieur à 100 EUR, la transaction devra être validée manuellement.

3.1. Gestion des risques et authentification 3D Secure

Le dispositif 3D Secure permet de réduire le risque d'impayés, grâce au transfert de responsabilité du marchand à la banque du titulaire de la carte. Voir chapitre [Onglet Résultat 3D Secure](#) à la page 13.

La gestion des risques avancée donne accès à des actions spécifiques lors du paramétrage des règles :

- "Définir un mode d'authentification" lorsque 3D Secure v2 est aussi activé sur au moins un des contrats associés à la boutique.

En fonction des protocoles disponibles sur son contrat, ces actions permettent au marchand :

- d'exprimer son souhait de challenger l'acheteur avec une authentification forte lors du paiement.

Les marchands autorisés peuvent, depuis les requêtes de paiement :

- demander une authentification 3D Secure v2 sans interaction du porteur ou frictionless si une exemption s'applique (voir : "[Application des exemptions](#)") et si la boutique dispose de l'option "Frictionless 3DS2").

Pour cela, ils utilisent le champ **strongAuthentication** de l'API REST ou le champ **vads_threeds_mpi** de l'API Formulaire.

Cette fonctionnalité peut être utilisée en complément du module de risques.

Dans ce cas, le paramètre transmis dans la requête de paiement est prioritaire sur les décisions du module de gestion des risques.

Application des exemptions :



Rappel :

En respect des règles des réseaux bancaires, une transaction réalisée sans authentification du porteur ne bénéficie pas du transfert de responsabilité.

D'autres règles peuvent s'appliquer en priorité sur celles définies par le marchand (dans ses requêtes de paiement ou depuis le module de gestion des risques) :

- Certaines cartes de paiement nécessitent une authentification du porteur. C'est le cas des cartes Maestro.
- American Express se réserve le droit d'effectuer une authentification forte en fonction de règles qui lui sont propres, même si le marchand a fait une configuration différente.


3.2. Les critères

Le marchand peut décider de modifier le processus de paiement en fonction de différents critères :

- Critères relatifs au montant.
Il s'agit des informations de la transaction (montant, devise, panier, acheteur, etc.).
- Critères relatifs à l'analyse de la carte.
Il s'agit du type de carte (Visa, Mastercard, etc.), du produit de la carte (personnelle, commerciale, prépayée), du pays émetteur, etc.
- Critères relatifs au résultat de 3D Secure.
Il s'agit de l'enrôlement du porteur, du statut de l'authentification.
- Critères relatifs aux pays.
Contrôle des différents pays : pays de facturation, pays de livraison, pays de la banque émettrice de la carte, etc.
- Critères de vélocité.
Il s'agit de critères qui évoluent en fonction de l'activité de la carte, de l'e-mail, etc. sur la boutique du marchand.

3.3. Les actions

Plusieurs actions sont mises à disposition :

Action	Description
Valider manuellement	<p>Cette action permet de bloquer temporairement la remise du paiement. Pendant ce temps, le marchand peut vérifier la transaction et décider de la valider ou l'annuler.</p> <p>La transaction est créée en validation manuelle. Elle peut être validée tant que le délai de remise en banque n'est pas dépassé. Passé ce délai, le paiement prend le statut "Expiré". Ce statut est définitif.</p> <p>Lorsque la transaction est créée en validation manuelle suite à l'application d'une règle de risque, le marchand est averti via la notification de fin de paiement.</p> <p>La valeur MANUAL_VALIDATION est transmise dans vads_risk_assessment_result en mode redirection et fraudManagement.riskAssessments.results en mode embarqué.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin: 10px 0;">  Le marchand ne peut pas définir de règle de notification spécifique pour être alerté de cette action. </div> <p>Cette action peut être cumulée avec d'autres actions, comme Remonter une alerte ou Définir un mode d'authentification.</p>
Refuser le paiement	<p>Cette action permet de refuser un paiement.</p> <p>Exemple : refuser un paiement si la carte utilisée est une carte commerciale.</p> <p>L'action Refuser est prioritaire sur l'action Valider manuellement.</p>
Remonter une alerte	<p>Cette action permet d'avertir le marchand qu'un risque est identifié.</p> <p>Exemple : le montant de la transaction est supérieur à 1000 EUR, la transaction a été réalisée avec une carte d'un pays jugé à risque.</p> <p>Cette action peut être cumulée avec d'autres actions, comme Valider manuellement ou Définir un mode d'authentification.</p> <p>L'alerte permet au marchand de déclencher des traitements ou des vérifications sur la transaction, comme par exemple, mettre en attente son processus de livraison le temps que des vérifications puissent être réalisées sur la transaction.</p> <p>Le marchand est averti :</p> <ul style="list-style-type: none"> • via la notification de fin de paiement ; La valeur INFORM est transmise dans vads_risk_assessment_result en mode redirection et fraudManagement.riskAssessments.results en mode embarqué. • par e-mail. Le marchand doit créer une règle de notification par e-mail spécifique afin de recevoir l'alerte. La condition pour déclencher la règle de notification est Gestion des risques informative = Échouée. Pour plus d'informations sur la procédure de configuration de la notification, voir : Créer des règles de notifications spécifiques à la gestion du risque à la page 39.
Définir un mode d'authentification.	<p>Cette action n'est disponible que si la 3D Secure v2 est activé sur au moins un des contrats associés à la boutique.</p>

Action	Description
	<p>Elle permet de modifier le mode d'authentification par défaut (NO_PREFERENCE) appliqué lors du paiement.</p> <p>Les choix disponibles dépendent des options de la boutique.</p> <p>Si votre boutique dispose de l'option "Frictionless 3DS2" et est associée à un contrat 3DS2 activé, vous aurez le choix entre les modes d'authentification suivants :</p> <ul style="list-style-type: none"> • Demande d'authentification avec interaction de l'acheteur (Challenge) ; • Demande d'authentification sans interaction de l'acheteur (Frictionless). <p>En choisissant le choix "Frictionless", l'authentification 3D Secure v2 sera réalisée avec une préférence marchand forcée à Frictionless si une exemption s'applique (voir : Application des exemptions).</p> <p>Pour plus d'informations, cliquez sur l'icône "?" présent dans la colonne Aide.</p> <p>Action non disponible dans l'onglet "Résultat 3D Secure".</p>

4. CONFIGURER LA GESTION DES RISQUES AVANCÉE

La gestion des risques avancée est accessible depuis le Back Office Marchand :

1. Connectez-vous à votre Back Office : <https://scelliuspaiement.labanquepostale.fr/vads-merchant/>.
2. Sélectionnez le menu **Paramétrage > Gestion des risques avancée**.

Si vous possédez plusieurs boutiques, sélectionnez une boutique.

Les contrôles sont regroupés par onglets :

- Configuration
- Résultat 3D Secure
- Montant
- Moyen de paiement
- Panier
- Pays
- Fréquence d'utilisation
- Media
- Résultat SafeKey

4.1. Onglet Configuration

L'onglet **Configuration** est donné à titre d'information et indique le "comportement 3D Secure par défaut" de la boutique. Le 3D Secure étant activé par défaut, le bouton **Sauvegarder** est grisé car le marchand ne peut pas modifier le comportement.

Si la carte est enrôlée 3D Secure v2, l'authentification est réalisée avec la préférence marchand "No preference". Dans ce cas, l'établissement bancaire émetteur décide du mode d'authentification le plus adapté en fonction des caractéristiques de la transaction.

Si la carte n'est pas enrôlée 3D Secure, il n'y a pas d'authentification préalable de l'acheteur et vous ne bénéficierez pas du transfert de responsabilité.

4.2. Onglet Résultat 3D Secure

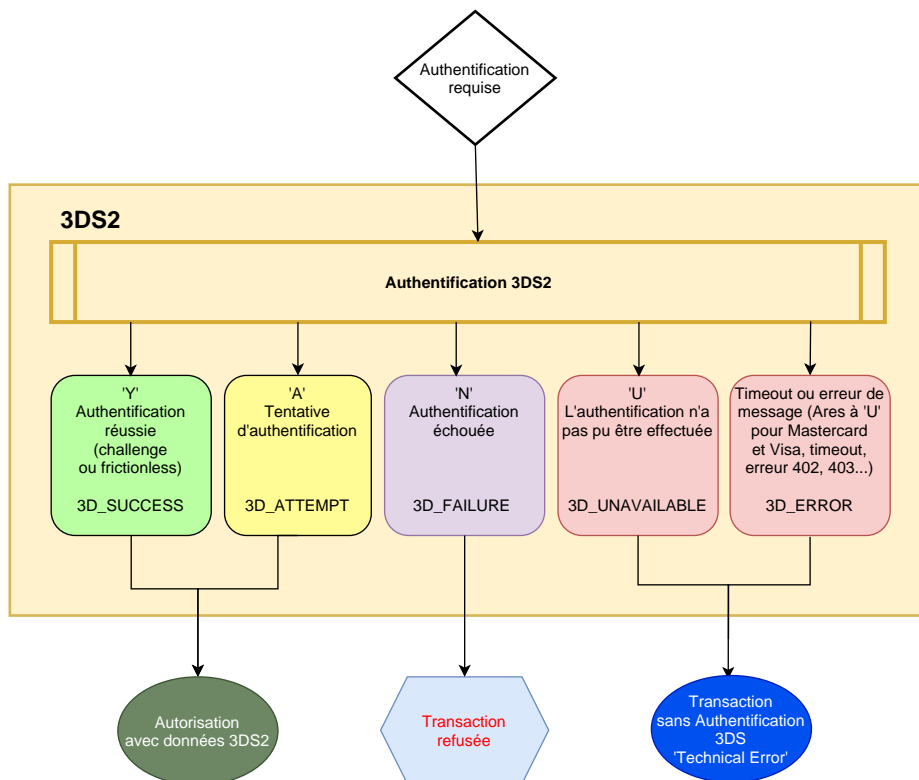
3D Secure, également nommé " Paiement sécurisé " chez CB, " Visa Secure " chez Visa, " Mastercard Identity check " chez Mastercard, " Safekey " chez American Express ou " ProtectBuy " chez Diners et Discover, est une norme internationale de protocole sécurisant les transactions en ligne.

Le principe du 3D Secure consiste à demander à l'acheteur, en plus de ses données bancaires habituelles (numéro de carte bancaire, mois et année d'expiration, cryptogramme si la carte en possède un), une information supplémentaire, indépendante de la carte, afin de s'assurer que l'acheteur est bien le titulaire du moyen de paiement. Dans la plupart des cas il s'agit d'un code confidentiel, à usage unique, communiqué par e-mail ou SMS à chaque nouvelle transaction. Si cette information n'est pas correctement renseignée par l'acheteur, la transaction prend fin.

Son objectif est de :

- réduire la fraude pour les marchands ;
- sécuriser les paiements pour les acheteurs.

Le schéma ci-dessous illustre le principe de l'authentification 3D Secure 2 :



4.2.1. Paiement 3D Secure avec un porteur dont l'authentification ne peut pas être vérifiée

Pour déclencher une ou plusieurs actions lorsque le statut de l'authentification du porteur ne peut pas être vérifié :

1. Cliquez sur le bouton **Activer**.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

3. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter**.

4. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

5. Cliquez sur **Sauvegarder** en bas de l'écran.

4.2.2. Carte non enrôlée au programme 3D Secure

Pour déclencher une ou plusieurs actions lorsque la transaction est réalisée avec une carte non enrôlée au programme 3D Secure :

1. Cliquez sur le bouton **Activer**.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

3. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter**.

4. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

5. Cliquez sur **Sauvegarder** en bas de l'écran.

4.2.3. Paiement 3D Secure avec une carte dont l'enrôlement ne peut pas être vérifié

Pour déclencher une ou plusieurs actions lorsque la transaction est réalisée avec une carte dont l'enrôlement au programme 3D Secure ne peut pas être vérifié suite à un dysfonctionnement de l'environnement 3D Secure :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

3. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

4. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

5. Cliquez sur Sauvegarder en bas de l'écran.

4.2.4. Transfert de responsabilité

Ce profil permet de déclencher une ou plusieurs actions lorsque la transaction ne bénéficie pas du transfert de responsabilité.

Les transactions bénéficiant du transfert de responsabilité sont les transactions pour lesquelles le porteur de carte ne peut pas transférer la responsabilité d'un impayé pour le motif « Contestation du porteur » vers le marchand.



Cette règle ne se déclenche pas si le 3D Secure n'est pas applicable sur la transaction (paiement MOTO par exemple).

Pour déclencher une ou plusieurs actions lorsque une transaction ne bénéficie pas du transfert de responsabilité :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Spécifiez un montant minimum et sa devise.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur Sauvegarder en bas de l'écran.

4.3. Onglet Montant

L'onglet **Montant** permet de déclencher une ou plusieurs actions en fonction du montant de la transaction.

4.3.1. Contrôle sur le montant

Il est possible d'activer un contrôle en fonction du montant du paiement.

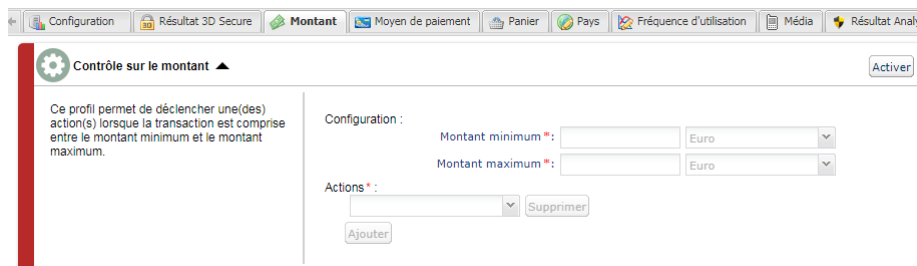


Image 1 : Onglet Montant

Pour cela :

1. Cliquez sur le bouton **Activer**.

Le bandeau vert indique que le profil est activé.

2. Spécifiez un montant minimum et maximum qui permettront de déclencher une action.
3. Spécifiez la devise qui s'applique au montant minimum et maximum.
Les devises appliquées doivent être les mêmes sinon le bouton **Sauvegarder** ne sera pas actif.
4. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.
Pour plus d'informations, voir : [Les actions](#) à la page 9.
5. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter**.
6. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.
7. Cliquez sur **Sauvegarder** en bas de l'écran.

4.3.2. Contrôle sur le montant minimum

Il est possible d'activer un contrôle en dessous d'un montant minimum.

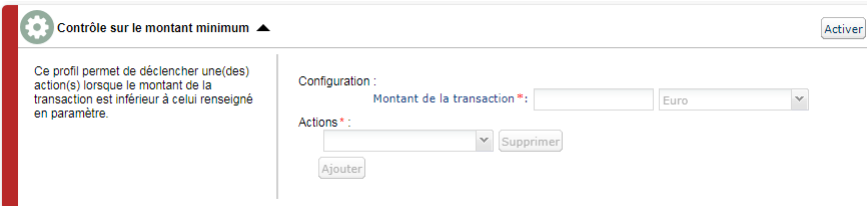
The screenshot shows a configuration window titled 'Contrôle sur le montant minimum' with a green gear icon and an 'Activer' button in the top right. The window is divided into two main sections. The left section contains a descriptive text: 'Ce profil permet de déclencher une(des) action(s) lorsque le montant de la transaction est inférieur à celui renseigné en paramètre.' The right section is labeled 'Configuration :'. It features a 'Montant de la transaction *' input field, a currency dropdown menu currently set to 'Euro', and an 'Actions *' dropdown menu. Below the 'Actions *' menu are two buttons: 'Ajouter' and 'Supprimer'.

Image 2 : Contrôle sur le montant minimum

1. Cliquez sur le bouton **Activer**.
Le bandeau vert indique que le profil est activé.
2. Spécifiez un montant de la transaction qui permettra de déclencher une action si le montant de la transaction est inférieur à celui renseigné.
3. Spécifiez la devise qui s'applique au montant minimum.
4. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.
Pour plus d'informations, voir : [Les actions](#) à la page 9.
5. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter**.
6. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.
7. Cliquez sur **Sauvegarder** en bas de l'écran.

4.3.3. Contrôle sur le montant maximum

Il est possible d'activer un contrôle à partir d'un montant maximum.



The screenshot shows a configuration window titled 'Contrôle sur le montant maximum' with a green 'Activer' button in the top right corner. On the left, a red vertical bar indicates the profile is active. The main content area is split into two sections: 'Configuration' and 'Actions'. The 'Configuration' section contains a text input field for 'Montant de la transaction*' and a dropdown menu set to 'Euro'. The 'Actions' section contains a dropdown menu and a 'Supprimer' button. At the bottom of the window, there is an 'Ajouter' button.

Image 3 : Contrôle sur le montant maximum

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Spécifiez un montant de la transaction qui permettra de déclencher une action si le montant de la transaction est supérieur à celui renseigné.

3. Spécifiez la devise qui s'applique au montant maximum.

4. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

5. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

6. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

7. Cliquez sur Sauvegarder en bas de l'écran.

4.3.4. Contrôle du montant cumulé pour un moyen de paiement sur une semaine

Il est possible d'activer un contrôle du montant cumulé payé avec un moyen de paiement sur une semaine.



Image 4 : Contrôle du montant cumulé

1. Cliquez sur le bouton **Activer.**

Le bandeau vert indique que le profil est activé.

2. Spécifiez un montant cumulé qui permettra de déclencher une action si le montant de la transaction fait atteindre le seuil fixé.

3. Spécifiez la devise qui s'applique au montant cumulé.

4. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

5. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter.**

6. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

7. Cliquez sur **Sauvegarder en bas de l'écran.**

4.4. Onglet Moyen de paiement

L'onglet **Moyen de paiement** permet de définir différents profils permettant de déclencher une ou plusieurs actions en fonction de la catégorie de la carte utilisée par l'acheteur.

4.4.1. Contrôle des cartes commerciales

Une carte commerciale est une carte de société. Elle est délivrée par exemple à un salarié à des fins professionnelles.

Pour déclencher une ou plusieurs actions lorsqu'un acheteur utilise une carte commerciale pour procéder à un paiement :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez une ou des marques de carte à contrôler.

Il est possible de sélectionner plusieurs cartes.

Les cartes contrôlées sont :

- CB ;
- VISA ;
- MASTERCARD ;
- MAESTRO ;
- ELECTRON ;
- VPAY.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur Sauvegarder en bas de l'écran.

4.4.2. Contrôle des cartes commerciales suivant leur provenance

Une carte commerciale est une carte de société. Elle est délivrée par exemple à un salarié à des fins professionnelles.

Pour déclencher une ou plusieurs actions lorsqu'un acheteur utilise une carte commerciale provenant d'un pays parmi ceux de la liste proposée pour procéder à un paiement :

1. Cliquez sur le bouton **Activer.**

Le bandeau vert indique que le profil est activé.

2. Sélectionnez un ou plusieurs pays en cliquant sur le bouton **Ajouter.**

Le ou les pays qui permettront de déclencher une action s'affichent dans la colonne **Pays sélectionnés**.

Cette liste n'est pas figée. Il est possible, à tout moment, de retirer l'un d'entre eux en le sélectionnant et en cliquant sur le bouton **Enlever**.

3. Sélectionnez une ou des marques de carte à contrôler.

Il est possible de sélectionner plusieurs cartes.

Les cartes contrôlées sont :

- CB ;
- VISA ;
- MASTERCARD ;
- MAESTRO ;
- ELECTRON ;
- VPAY.

4. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

5. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter.**

6. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

7. Cliquez sur **Sauvegarder en bas de l'écran.**

4.4.3. Contrôle des cartes prépayées

Une carte prépayée est un moyen de paiement qui s'apparente à un porte-monnaie électronique. Seules les sommes rechargées peuvent être dépensées (aucun risque de dépassement, de piratage de compte bancaire...).

Pour déclencher une ou plusieurs actions lorsqu'un acheteur utilise une carte prépayée pour procéder à un paiement :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez une ou des marques de carte à contrôler.

Il est possible de sélectionner plusieurs cartes.

Les cartes contrôlées sont :

- CB ;
- VISA ;
- MASTERCARD ;
- MAESTRO ;
- ELECTRON ;
- VPAY.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur Sauvegarder en bas de l'écran.

4.4.4. Contrôle des cartes à autorisation systématique

La carte à autorisation systématique est une carte de paiement. A chaque utilisation, le solde du compte est consulté et l'opération n'est autorisée que si la provision est suffisante.

Pour déclencher une ou plusieurs actions lorsqu'un acheteur utilise une carte Visa ou Mastercard à autorisation systématique pour procéder à un paiement :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez MAESTRO ou VISA_ELECTRON dans la liste des types de carte qui déclencherà une ou plusieurs actions.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Si vous souhaitez sélectionner un autre type de carte, réitérez les étapes 2 et 3 et selon vos besoins les étapes 4 et 5.

7. Cliquez sur Sauvegarder en bas de l'écran.

4.4.5. Contrôle des e-Carte-Bleue

Une e-Carte Bleue est une carte virtuelle qui fournit un numéro de carte éphémère pour chaque transaction réalisée sur Internet. Ainsi un numéro de carte bancaire « réel » ne transite pas sur Internet.

Pour déclencher une ou plusieurs actions lorsqu'un acheteur utilise une e-Carte-Bleue pour procéder à un paiement :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

3. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

4. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

5. Cliquez sur Sauvegarder en bas de l'écran.

4.4.6. Contrôle des cartes personnelles de crédit

Une carte personnelle de crédit est une carte de paiement. Le compte est débité en différé de la totalité des achats effectués pendant une période définie.

Pour déclencher une ou plusieurs actions lorsqu'un acheteur utilise une carte personnelle de crédit pour procéder à un paiement :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez une ou des marques de carte à contrôler.

Il est possible de sélectionner plusieurs cartes.

Les cartes contrôlées sont :

- CB ;
- VISA ;
- MASTERCARD ;
- MAESTRO ;
- ELECTRON ;
- VPAY.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur Sauvegarder en bas de l'écran.

4.4.7. Contrôle des cartes personnelles de débit

Une carte personnelle de débit est une carte de paiement. Le compte est prélevé au fur et à mesure que les transactions sont transmises par les marchands bénéficiaires.

Pour déclencher une ou plusieurs actions lorsqu'un acheteur utilise une carte personnelle de débit pour procéder à un paiement :

1. Cliquez sur le bouton **Activer.**

Le bandeau vert indique que le profil est activé.

2. Sélectionnez une ou des marques de carte à contrôler.

Il est possible de sélectionner plusieurs cartes.

Les cartes contrôlées sont :

- CB ;
- VISA ;
- MASTERCARD ;
- MAESTRO ;
- ELECTRON ;
- VPAY.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter.**

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur **Sauvegarder en bas de l'écran.**

4.5. Onglet Panier

L'onglet **Panier** permet de définir différents profils permettant de déclencher une ou plusieurs actions en fonction du contenu du panier de l'acheteur.

4.5.1. Contrôle sur le nombre de produits du panier

Pour déclencher une ou plusieurs actions lorsqu'un acheteur totalise un certain nombre de produits dans le panier lorsqu'il effectue son paiement :

1. Cliquez sur le bouton **Activer.**

Le bandeau vert indique que le profil est activé.

2. Spécifiez le nombre de produits qui permettra de déclencher une ou plusieurs actions.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter.**

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur **Sauvegarder en bas de l'écran.**

4.5.2. Contrôle des produits du panier

Pour déclencher une ou plusieurs actions lorsqu'un acheteur possède un ou plusieurs codes produits spécifiques dans son panier :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Spécifiez un code produit pour lequel vous souhaitez déclencher une ou plusieurs actions.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Si vous souhaitez ajouter un autre code produit, réitérez l'étape 2 en séparant les codes produit par un ";".

7. Cliquez sur Sauvegarder en bas de l'écran.

4.6. Onglet Pays

L'onglet **Pays** permet de définir différents profils permettant de déclencher une ou plusieurs actions en fonction d'un ou plusieurs pays liés à la transaction.

4.6.1. Contrôle du pays de l'acheteur (adresse de facturation)

Tous les pays sont acceptés par défaut. L'expression « Pays de l'acheteur » indique le pays de l'adresse de facturation.

Pour déclencher une ou plusieurs actions pour protéger un site marchand contre des risques spécifiques liés à un ou plusieurs pays :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez un ou plusieurs pays en cliquant sur le bouton Ajouter.

Le ou les pays qui permettront de déclencher une action s'affichent dans la colonne **Pays sélectionnés**.

Cette liste n'est pas figée. Il est possible, à tout moment, de retirer l'un d'entre eux en le sélectionnant et en cliquant sur le bouton **Enlever**.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur Sauvegarder en bas de l'écran.

4.6.2. Contrôle du pays de livraison

Tous les pays sont acceptés par défaut.

Pour déclencher une ou plusieurs actions pour protéger un site marchand contre des risques spécifiques liés à un ou plusieurs pays :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez un ou plusieurs pays en cliquant sur le bouton Ajouter.

Le ou les pays qui permettront de déclencher une action s'affichent dans la colonne **Pays sélectionnés**.

Cette liste n'est pas figée. Il est possible, à tout moment, de retirer l'un d'entre eux en le sélectionnant et en cliquant sur le bouton **Enlever**.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur Sauvegarder en bas de l'écran.

4.6.3. Contrôle de la variété des pays

Une ou plusieurs actions peuvent être déclenchée(s) lorsque le nombre de pays concernés par la transaction dépasse un certain seuil et le montant de la transaction est compris entre un montant minimum et maximum.

Lorsque ce cas de figure se présente, un contrôle est réalisé sur la base des critères suivants :

- le pays correspondant à l'adresse de l'acheteur ;
- le pays de l'adresse de livraison ;
- le pays de l'IP utilisée lors du paiement ;
- le pays de la carte.

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Définissez le seuil de pays (1, 2, 3 ou 4) qui déclenche une ou plusieurs actions.

3. Spécifiez un montant minimum et maximum qui permettront de déclencher une action.

4. Spécifiez la devise qui s'applique au montant minimum et maximum.

Les devises appliquées doivent être les mêmes sinon le bouton **Sauvegarder** ne sera pas actif.

5. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

6. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

7. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

8. Cliquez sur Sauvegarder en bas de l'écran.

4.6.4. Contrôle sur des produits carte provenant de certains pays

Ce profil permet de déclencher une ou plusieurs actions lorsque :

- le type de produit carte est parmi ceux sélectionnés (carte prépayée, carte commerciale, carte personnelle) ;
- et que le pays de la carte soit parmi la liste des pays sélectionnés.

Pour déclencher une ou plusieurs actions :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez un ou plusieurs types de produit dans la liste proposée.

Les valeurs possibles sont les suivantes :

- **Carte prépayée**

Une carte prépayée est un moyen de paiement qui s'apparente à un porte-monnaie électronique. Seules les sommes rechargées peuvent être dépensées (aucun risque de dépassement, de piratage de compte bancaire, etc.).

- **Carte commerciale**

Une carte commerciale est une carte de société. Elle est délivrée par exemple à un salarié à des fins professionnelles.

- **Carte personnelle**

Une carte personnelle est une carte bancaire délivrée à un particulier pour son usage personnel.

3. Sélectionnez un ou plusieurs pays en cliquant sur le bouton Ajouter.

Le ou les pays qui permettront de déclencher une action s'affichent dans la colonne **Pays sélectionnés**.

Cette liste n'est pas figée. Il est possible, à tout moment, de retirer l'un d'entre eux en le sélectionnant et en cliquant sur le bouton **Enlever**.

4. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

5. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

6. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

7. Cliquez sur Sauvegarder en bas de l'écran.

4.6.5. Contrôle des pays pour les paiements SDD

Ce profil permet de déclencher des actions lorsque le pays du compte bancaire (IBAN) fait partie de la liste de pays sélectionnés.

Tous les pays sont acceptés par défaut.

Pour déclencher une ou plusieurs actions :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez un ou plusieurs pays en cliquant sur le bouton Ajouter.

Le ou les pays qui permettront de déclencher une action s'affichent dans la colonne **Pays sélectionnés**.

Cette liste n'est pas figée. Il est possible, à tout moment, de retirer l'un d'entre eux en le sélectionnant et en cliquant sur le bouton **Enlever**.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur Sauvegarder en bas de l'écran.

4.7. Onglet Fréquence d'utilisation

L'onglet **Fréquence d'utilisation** permet de définir différents profils permettant de déclencher une ou plusieurs actions en fonction de la fréquence d'utilisation d'un même moyen de paiement sur une semaine.

4.7.1. Fréquence d'utilisation d'une adresse e-mail sur une semaine

Pour déclencher une ou plusieurs actions lorsque de multiples tentatives de paiement sont détectées avec une adresse e-mail identique sur une semaine :

1. Cliquez sur le bouton **Activer**.

Le bandeau vert indique que le profil est activé.

2. Déterminez le nombre de tentatives de paiement effectué avec une même adresse e-mail pour déclencher une ou plusieurs actions.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter**.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur **Sauvegarder** en bas de l'écran.

4.7.2. Fréquence d'utilisation d'une adresse IP sur une semaine

Pour déclencher une ou plusieurs actions lorsque de multiples tentatives de paiement sont détectées avec une adresse IP identique sur une semaine :

1. Cliquez sur le bouton **Activer**.

Le bandeau vert indique que le profil est activé.

2. Déterminez le nombre de tentatives de paiement effectué avec une même adresse IP pour déclencher une ou plusieurs actions.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter**.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur **Sauvegarder** en bas de l'écran.

4.7.3. Fréquence d'utilisation d'un moyen de paiement sur une semaine



Le contrôle effectué s'applique aux numéros de cartes de paiement mais aussi aux numéros de compte bancaire servant lors de virement.

Pour déclencher une ou plusieurs actions lorsque de multiples tentatives de paiement sont détectées avec un numéro de carte identique sur une semaine :

1. Cliquez sur le bouton **Activer**.

Le bandeau vert indique que le profil est activé.

2. Déterminez le nombre de tentatives de paiement maximum à effectuer avec un même numéro de carte avant déclencher une ou plusieurs actions.

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton **Ajouter**.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur **Sauvegarder** en bas de l'écran.

4.8. Onglet Media

L'onglet **Media** permet de définir une ou plusieurs actions à réaliser en fonction du type d'équipement utilisé lors du paiement.

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez le ou les types d'équipement parmi la liste proposée: "Ordinateur, Tablette, Téléphone mobile".

3. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

4. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

5. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

6. Cliquez sur Sauvegarder en bas de l'écran.

4.9. Onglet Résultat SafeKey

American Express SafeKey est un outil d'authentification 3D Secure qui vise à réduire la fraude en ligne par l'authentification du porteur de la carte American Express à l'aide d'un code d'authentification.

4.9.1. Carte non enrôlée au programme SafeKey

Pour déclencher une ou plusieurs actions lorsque la transaction est réalisée avec une carte non enrôlée au programme SafeKey :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

3. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

4. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

5. Cliquez sur Sauvegarder en bas de l'écran.

4.9.2. Paiement avec une carte dont l'enrôlement au programme SafeKey ne peut pas être vérifié

Pour déclencher une ou plusieurs actions lorsque la transaction est réalisée avec une carte dont l'enrôlement au programme SafeKey d'American Express ne peut pas être vérifié suite à un dysfonctionnement de leur Directory Server :

1. Cliquez sur le bouton Activer.

Le bandeau vert indique que le profil est activé.

2. Sélectionnez l'action que vous souhaitez déclencher lorsque ce profil se présente.

Pour plus d'informations, voir : [Les actions](#) à la page 9.

3. Si vous souhaitez définir une ou plusieurs autres actions, cliquez sur le bouton Ajouter.

4. Sélectionnez l'action suivante que vous souhaitez déclencher lorsque ce profil se présente.

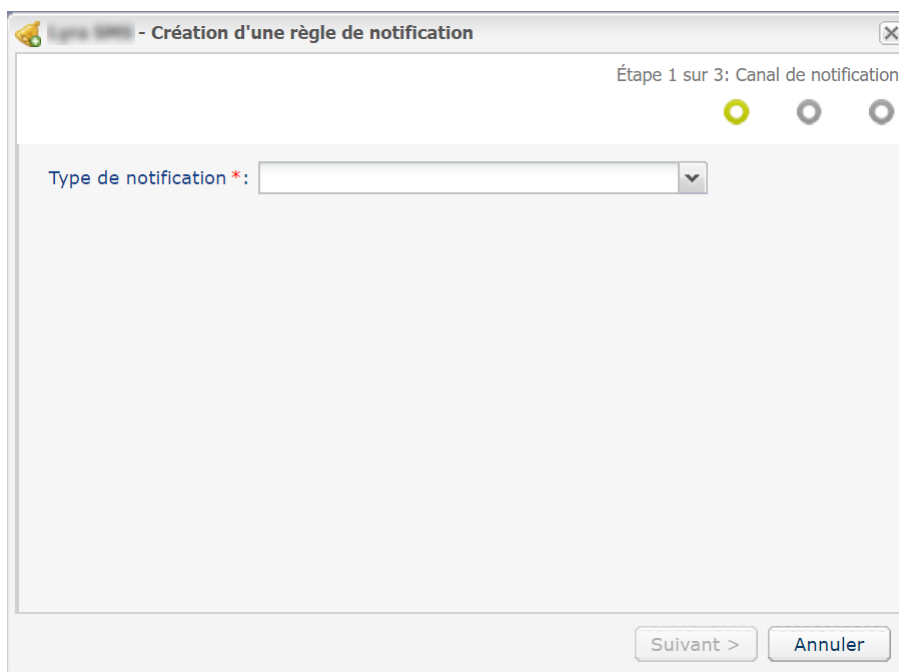
5. Cliquez sur Sauvegarder en bas de l'écran.

5. CRÉER DES RÈGLES DE NOTIFICATIONS SPÉCIFIQUES À LA GESTION DU RISQUE

Cas d'utilisation : L'action d'un contrôle de risque est configurée à **Relever une alerte**. Le marchand souhaite recevoir un e-mail dès lors qu'un contrôle détecte un risque de fraude.

Pour créer la règle de notification associée :

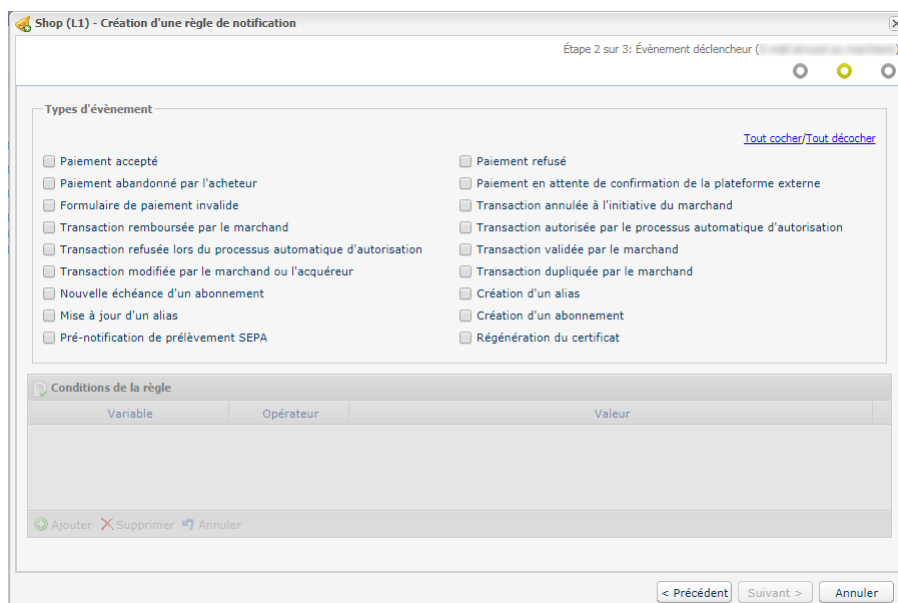
1. Depuis votre Back Office Marchand, allez dans le menu : **Paramétrage > Règles de notifications**.
2. Cliquez sur le bouton **Créer une règle** situé en bas à gauche de l'écran.
3. Sélectionnez **Notification avancée**.



The screenshot shows a window titled "Création d'une règle de notification" with a progress indicator showing "Étape 1 sur 3: Canal de notification". The first step is active, indicated by a yellow circle. Below the progress indicator, there is a dropdown menu labeled "Type de notification *:". At the bottom right, there are two buttons: "Suivant >" and "Annuler".

4. Sélectionnez le type de notification **E-mail envoyé au marchand**.

5. Cliquez sur **Suivant**.



The screenshot shows the same window at "Étape 2 sur 3: Événement déclencheur". The second step is active, indicated by a yellow circle. Under the heading "Types d'événement", there is a list of 16 events, each with a checkbox. A link "Tout cocher/Tout décocher" is visible on the right. Below this list is a section titled "Conditions de la règle" with a table structure for defining conditions. At the bottom, there are buttons for "Ajouter", "Supprimer", and "Annuler". At the very bottom of the window, there are navigation buttons: "< Précédent", "Suivant >", and "Annuler".

Variable	Opérateur	Valeur
----------	-----------	--------

6. Cochez les événements déclencheurs en fonction de votre besoin.

Exemple : **Paiement refusé**, **Paiement accepté** et **Création d'alias**.

7. Dans la section **Conditions de la règle**, cliquez sur **Ajouter**.

8. Dans la colonne **Variable**, sélectionnez **Gestion des risques informative**.

9. Sélectionnez l'opérateur **égal à**.

10. Sélectionnez la valeur **Échoués**.

11. Cliquez sur **Suivant**.

12. Renseignez le **Libellé de la règle**.

13. Renseignez l'adresse e-mail à notifier.

14. Choisissez les champs à inclure dans l'e-mail.

Par défaut, le détail du module de gestion de risques avancée est déjà inclus.

15. Si vous souhaitez modifier le contenu du message, cliquez sur **Personnaliser des valeurs de texte par défaut**, dans la section **Paramétrage e-mail**.

16. Une fois le paramétrage achevé, cliquez sur **Créer**.

Lorsqu'une règle de risque configurée avec l'action **Relever une alerte** se déclenche, le marchand reçoit un e-mail contenant le détail de l'appel au module de gestion des risques avancée :

Détail de l'appel au module de gestion des risques avancée

 **Lever une alerte**

6. TRANSMETTRE LES DONNÉES UTILES À LA GESTION DES RISQUES AVANCÉE

Pour réaliser les contrôles activés et configurés dans le Back Office Marchand, la demande de paiement doit contenir les données à analyser.

Pour cette raison, le marchand doit :

- Transmettre les données de la commande pour connaître le détails du panier ;
- Transmettre les données de l'acheteur pour connaître le pays de la facturation (vads_cust_country / customer.billingDetails.country) ;
- Transmettre les données de livraison pour connaître le pays de la livraison (vads_ship_to_country / customer.shippingDetails.country).

6.1. Transmettre les données de la commande

Le marchand peut indiquer dans son formulaire de paiement s'il souhaite transmettre les informations de la commande (numéro de la commande, description, contenu du panier etc.).

Pour déclencher une ou plusieurs actions en fonction du contenu du panier de l'acheteur, les données du panier doivent obligatoirement être transmises dans la requête de paiement.

Ces données seront affichées dans le Back Office Marchand en consultant le détail de la transaction (onglet **Panier**).

Nom du champ	Description	Valeur
API Formulaire : vads_order_id API REST : orderId	Numéro de commande	Ex : 2-XQ001
API Formulaire : vads_order_info API REST : metadata.orderInfo1	Informations complémentaires sur la commande	Ex : Code interphone 3125
API Formulaire : vads_order_info2 API REST : metadata.orderInfo2	Informations complémentaires sur la commande	Ex : Sans ascenseur
API Formulaire : vads_order_info3 API REST : metadata.orderInfo3	Informations complémentaires sur la commande	Ex : Express
API Formulaire : vads_nb_products API REST : N/A	Nombre d'articles présents dans le panier	Ex : 2
API Formulaire : vads_product_ext_idN API REST : N/A	Code barre du produit dans le site web du marchand. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...)	Ex : 0123654789123654789
API Formulaire : vads_product_labelN API REST : cartItemInfo.productLabel	Libellé de l'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...).	Ex : Séjour 3 jours datés
API Formulaire : vads_product_amountN API REST : cartItemInfo.productLabel	Montant de l'article exprimé dans la plus petite unité de la devise. N correspond à l'indice de l'article	Ex : 32150

Nom du champ	Description	Valeur
	(0 pour le premier, 1 pour le second...).	
API Formulaire : vads_product_typeN API REST : cartItemInfo.productType	Type de l'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...). Consultez le tableau des valeurs ci-après.	Ex : TRAVEL
API Formulaire : vads_product_refN API REST : cartItemInfo.productRef	Référence de l'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...).	Ex : 1002127784
API Formulaire : vads_product_qtyN API REST : cartItemInfo.productQty	Quantité d'article. N correspond à l'indice de l'article (0 pour le premier, 1 pour le second...).	Ex : 1

Type de l'article (vads_product_type / productType)

Valeur	Description
FOOD_AND_GROCERY	Produits alimentaires et d'épicerie
AUTOMOTIVE	Automobile / Moto
ENTERTAINMENT	Divertissement / Culture
HOME_AND_GARDEN	Maison / Jardin
HOME_APPLIANCE	Équipement de la maison
AUCTION_AND_GROUP_BUYING	Ventes aux enchères / Achats groupés
FLOWERS_AND_GIFTS	Fleurs / Cadeaux
COMPUTER_AND_SOFTWARE	Ordinateurs / Logiciels
HEALTH_AND_BEAUTY	Santé / Beauté
SERVICE_FOR_INDIVIDUAL	Services à la personne
SERVICE_FOR_BUSINESS	Services aux entreprises
SPORTS	Sports
CLOTHING_AND_ACCESSORIES	Vêtements / Accessoires
TRAVEL	Voyage
HOME_AUDIO_PHOTO_VIDEO	Son / Image / Vidéo
TELEPHONY	Téléphonie

6.2. Transmettre les données de l'acheteur

Les informations de l'acheteur (adresse e-mail, civilité, numéro de téléphone, etc.) constituent les informations de facturation.

Toutes les données transmises sont affichées dans le détail de la transaction (onglet **Acheteur**) dans le Back Office Marchand.

Nom du champ	Description	Valeur
API Formulaire : vads_cust_email API REST : customer.email	Adresse e-mail de l'acheteur	Ex: abc@example.com
API Formulaire : vads_cust_id API REST : customer.reference	Référence de l'acheteur sur le site marchand	Ex: C2383333540
API Formulaire : vads_cust_title API REST : customer.billingDetails.title	Civilité de l'acheteur	Ex : Monsieur
API Formulaire : vads_cust_status API REST : customer.billingDetails.category	Statut	PRIVATE : pour un particulier COMPANY : pour une entreprise
API Formulaire : vads_cust_first_name API REST : customer.billingDetails.firstName	Prénom	Ex : Laurent
API Formulaire : vads_cust_last_name API REST : customer.billingDetails.lastName	Nom	Ex : Durant
API Formulaire : vads_cust_legal_name API REST : customer.billingDetails.legalName	Raison sociale de l'acheteur	Ex : D. & Cie
API Formulaire : vads_cust_cell_phone API REST : customer.billingDetails.cellPhoneN	Numéro de téléphone mobile	Ex : 06 12 34 56 78
API Formulaire : vads_cust_address_number API REST : customer.billingDetails.streetNumb	Numéro de rue	Ex : 109
API Formulaire : vads_cust_address API REST : customer.billingDetails.address	Adresse postale	Ex : Rue de l'innovation
API Formulaire : vads_cust_address2 API REST : customer.billingDetails.address2	Deuxième ligne d'adresse	Ex :
API Formulaire : vads_cust_district API REST : customer.billingDetails.district	Quartier	Ex: Centre ville
API Formulaire : vads_cust_zip	Code postal	Ex : 31670

Nom du champ	Description	Valeur
API REST : customer.billingDetails.zipcode		
API Formulaire : vads_cust_city API REST : customer.billingDetails.city	Ville	Ex : Labège
API Formulaire : vads_cust_state API REST : customer.billingDetails.state	Etat / Région	Ex : Occitanie
API Formulaire : vads_cust_country API REST : customer.billingDetails.country	Code pays suivant la norme ISO 3166 alpha-2. Doit obligatoirement être transmis pour déclencher une ou plusieurs actions en fonction du pays de l'acheteur.	Ex : "FR" pour la France, "PF" pour la Polynésie Française, "NC" pour la Nouvelle Calédonie, "US" pour les Etats-Unis.

Les champs **vads_cust_phone** et **vads_cust_cell_phone** acceptent tous les formats. Exemples :



- 0123456789
- +33123456789
- 0033123456789
- (00.571) 638.14.00
- 40 41 42 42

6.3. Transmettre les données de livraison

Les données de livraison de l'acheteur sont l'adresse, la civilité, le numéro de téléphone, etc..

Ces données seront affichées dans le Back Office Marchand en consultant le détail de la transaction (onglet **Livraison**).

Nom du champ	Description	Valeur
API Formulaire : vads_ship_to_city API REST : customer.shippingDetails.city	Ville	Ex : Bordeaux
API Formulaire : vads_ship_to_country API REST : customer.shippingDetails.country	Code pays suivant la norme ISO 3166. Doit obligatoirement être transmis pour déclencher une ou plusieurs actions si le profil Contrôle du pays de la livraison est activé.	Ex : FR
API Formulaire : vads_ship_to_district API REST : customer.shippingDetails.district	Quartier	Ex : La Bastide
API Formulaire : vads_ship_to_first_name API REST : customer.shippingDetails.firstName	Prénom	Ex : Albert
API Formulaire : vads_ship_to_last_name API REST : customer.shippingDetails.lastName	Nom	Ex : Durant
API Formulaire : vads_ship_to_legal_name API REST : customer.shippingDetails.legalName	Raison sociale	Ex : D. & Cie
API Formulaire : vads_ship_to_phone_num API REST : customer.shippingDetails.phoneNum	Numéro de téléphone	Ex: 0460030288
API Formulaire : vads_ship_to_state API REST : customer.shippingDetails.state	Etat / Région	Ex : Nouvelle aquitaine
API Formulaire : vads_ship_to_status API REST : customer.shippingDetails.status	Définit le type d'adresse de livraison	PRIVATE : pour une livraison chez un particulier COMPANY : pour une livraison en entreprise
API Formulaire : vads_ship_to_street_number API REST : customer.shippingDetails.streetNum	Numéro de rue	Ex : 2
API Formulaire : vads_ship_to_street	Adresse postale	Ex : Rue Sainte Catherine

Nom du champ	Description	Valeur
API REST : customer.shippingDetails.address		
API Formulaire : vads_ship_to_street2 API REST : customer.shippingDetails.address2	Deuxième ligne d'adresse	
API Formulaire : vads_ship_to_zip API REST : customer.shippingDetails.zipCode	Code postal	Ex : 33000

Le champ **vads_ship_to_phone_num** accepte tous les formats. Exemples :



- 0123456789
- +33123456789
- 0033123456789
- (00.571) 638.14.00
- 40 41 42 42

7. CONSULTER LE DÉTAIL D'UNE TRANSACTION DANS LE BACK OFFICE MARCHAND

Les transactions sont visibles depuis le menu **Gestion > Transactions**.

Pour visualiser le détail d'une transaction :

1. Sélectionnez une transaction.
2. Effectuez un clic droit puis sélectionnez **Afficher le détail de la transaction**.
La boîte de dialogue **Détail d'une transaction** apparaît.
Le contenu de l'onglet **Informations** s'affiche par défaut.
Dans le groupe **Cycle de vie de la transaction**, le statut de la transaction est spécifié.

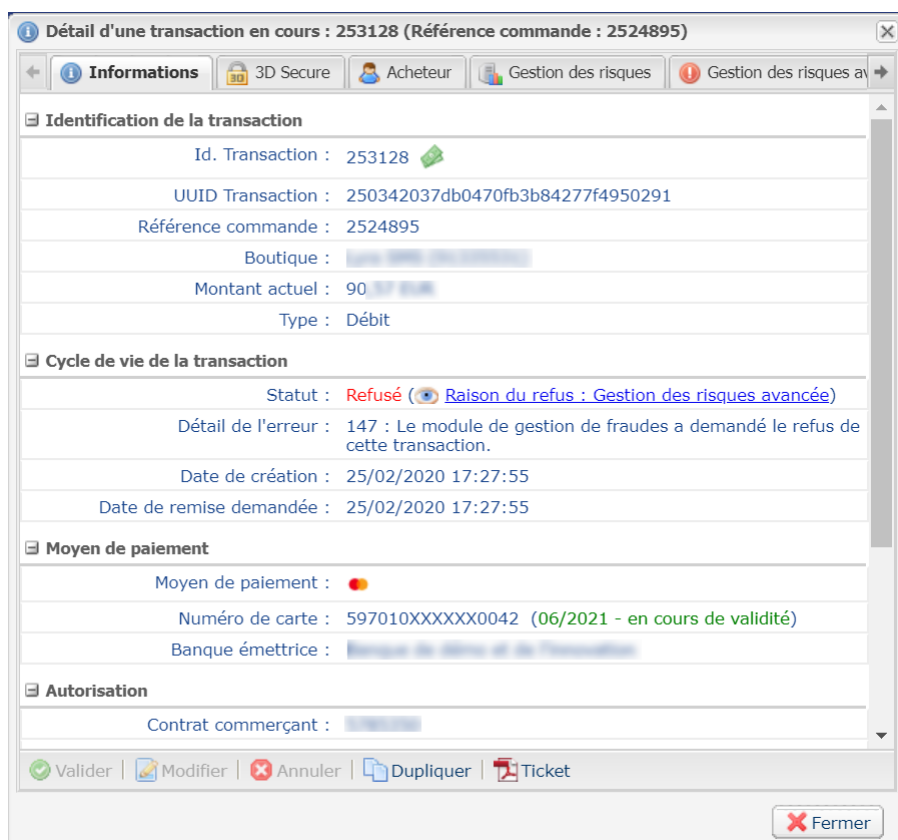


Image 5 : Onglet Informations

3. Cliquez sur l'onglet **Gestion des risques avancée** pour identifier la règle appliquée ainsi que l'action exécutée.

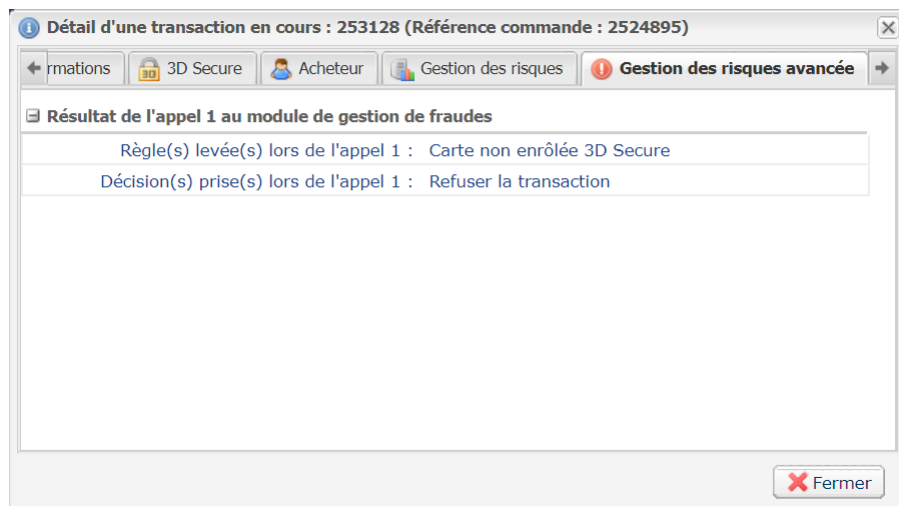


Image 6 : Onglet Gestion des risques avancée

8. VALIDER MANUELLEMENT UNE TRANSACTION

Si le marchand a opté pour une validation manuelle de la transaction lorsqu'il a paramétré un profil, celui-ci devra valider le paiement ultérieurement dans son Back Office.

Pour cela :

1. Effectuez un clic droit sur une transaction dont le statut est **A valider**.
2. Sélectionnez **Valider**.
3. Confirmez que vous souhaitez réellement valider la transaction sélectionnée.

9. RESTITUTION DU RÉSULTAT DU MODULE DE GESTION DES RISQUES AVANCÉE DANS L'IPN

Les actions renvoyées par le module de gestion des risques avancée sont retournées dans l'IPN via les champs:

- **vads_risk_assessment_result** pour l'API Formulaire
- **fraudManagement.riskAssessments.results** pour l'API REST

Les différentes valeurs possibles sont les suivantes :

Valeurs	Description
ENABLE_3DS	<ul style="list-style-type: none">• Le module de risque a demandé une authentification avec interaction du porteur (challenge).
DISABLE_3DS	<ul style="list-style-type: none">• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).
NO_PREFERENCE	<ul style="list-style-type: none">• Le module de risque a demandé une authentification 3DS. Le choix de la préférence est délégué à l'émetteur de la carte.
NO_CHALLENGE_REQUESTED	<ul style="list-style-type: none">• Le module de risque a demandé une authentification sans interaction du porteur (frictionless).
CHALLENGE_REQUESTED	<ul style="list-style-type: none">• Le module de risque a demandé une authentification avec interaction du porteur (challenge).
CHALLENGE_MANDATE	<ul style="list-style-type: none">• Le module de risque a demandé une authentification avec interaction du porteur (challenge) pour des raisons réglementaires.
MANUAL_VALIDATION	La transaction est créée en validation manuelle. La remise du paiement est bloquée temporairement pour permettre au marchand de procéder à toutes les vérifications souhaitées.
REFUSE	La transaction est refusée.
RUN_RISK_ANALYSIS	Appel à un analyseur de risques externe sous condition que le marchand possède un contrat. Se référer à la description de l'objet TransactionDetails.FraudManagement.RiskAnalysis pour identifier la liste des valeurs possibles et leur description.
INFORM	Une alerte est remontée. Le marchand est averti qu'un risque est identifié. Le marchand est informé via une ou plusieurs des règles du centre de notification (URL de notification, e-mail ou SMS).

10. OBTENIR DE L'AIDE

Vous cherchez de l'aide ? Consultez notre FAQ :

<https://scelliuspaiement.labanquepostale.fr/doc/fr-FR/faq/faq-homepage.html>

Pour toute question technique ou demande d'assistance, contactez [le support technique](#).

Pour faciliter le traitement de vos demandes, préparez votre identifiant de boutique (numéro à 8 chiffres).

Cette information est disponible dans l'e-mail d'inscription de votre boutique ou dans le Back Office Marchand (menu **Paramétrage** > **Boutique** > **Configuration**).