

# SYSTEME DE DETECTION ET D'ALERTE CONTRE LES FRAUDES DE PAIEMENT



Accès aux rapports  
et interface de pilotage

**Système compatible  
avec les plate-formes**



Pour plus d'informations:

**aouka**

Tél: +33 (6) 08 91 80 08  
+33 (6) 76 96 96 21

infos@aouka.com

www.aouka.com

A partir des journaux de fonds listant les transactions réalisées sur le site marchand du client, le système de détection de fraudes analyse quotidiennement la cohérence des données et alerte le client en cas de transactions suspectes.

## ANALYSE DES JOURNAUX

### - Offre de base:

Dans cette configuration les tests de cohérence porte exclusivement sur les pays. **La transaction a-t-elle été effectuée depuis le même pays que celui de la carte bancaire?**

### - Options:

> en modifiant le module de paiement du client, un test de cohérence supplémentaire sur **le pays de livraison** peut être mis en place.

> en modifiant le module de paiement du client, un test de cohérence supplémentaire sur **le code postal de livraison** peut être mis en place.

## SYSTEME D'ALERTE

Lors de la détection de transactions suspectes, **le client est alerté par courrier électronique**. Le tableau récapitulatif des transactions comportent les numéros de commande et de transaction afin de permettre au client d'annuler la transaction dans son interface backoffice bancaire et d'annuler la commande dans l'interface backoffice de sa boutique en ligne.

Le client peut également créer des alertes personnalisées en mettant sur «*liste noire*» des adresses IP, des pays d'origine de la transaction (déduit à partir de l'adresse IP) et des pays de carte bancaire.

## ACCES AU SITE

Le système permet également d'empêcher en amont les tentatives de fraudes. En incluant **une simple ligne de code HTML** sur les pages sensibles (typiquement la page de commande du site marchand du client), les utilisateurs suspects ne peuvent accéder au module de paiement.

Le filtre porte sur l'adresse IP et le pays de l'internaute (déduit de l'IP).

Ce filtre permet ainsi au commerçant de bloquer l'accès au module de paiement pour des internautes situés dans des zones où le client ne livre pas.

## SECURITE ET CONFIDENTIALITE

Les fichiers envoyés au serveur d'analyse ne sont pas conservés. Seules les données concernées par les tests sont stockées.

L'accès aux rapports d'analyse et au système se fait via une connexion HTTPS.