

Lyra

FRAUDE

**Comment lutter
efficacement pour
protéger son activité ?**

E-COMMERCE & IN-STORE

1 CONTEXTE DE LA FRAUDE

P.3

2 LA FRAUDE AU MOYEN DE PAIEMENT

P.4

3 L'ENJEU D'UN COMMERÇANT

P.5

4 QU'EST-CE QU'UN CHARGEBACK ?

P.6

5 L'OBJECTIF DES FRAUDEURS

P.7

6 COMMENT SE PROTÉGER ?

P.8

7 LES DIFFÉRENTS SCÉNARIOS

P.10

CONTEXTE DE LA FRAUDE.

Chaque année, des milliers de commerçants voient des paiements pourtant validés se transformer en pertes bien réelles. Une transaction acceptée ne garantit pas toujours un paiement effectif : fraude et chargebacks peuvent rapidement doubler le coût d'une vente et ébranler la rentabilité d'une activité.

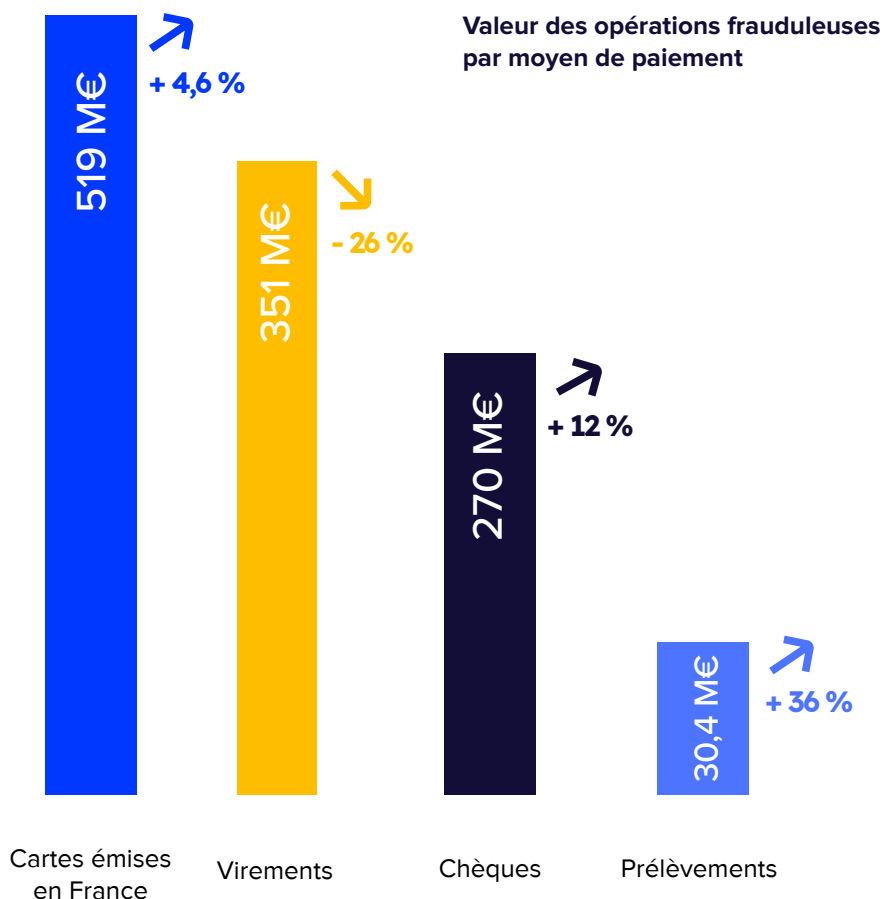
D'après l'Observatoire de la sécurité des moyens de paiement (OSMP), la fraude en France représente **1,2 milliard d'euros en 2024 pour 7,8 millions de transactions**.

La carte, moyen de paiement principal du quotidien, constitue **40,2% des cas de fraude en valeur et 94% en volume**. Le virement suivi du chèque et du prélèvement, représentent respectivement en valeur 29,5% (350M€) , 22.7% (270M€) et 2,6% (30M€). Des chiffres qui démontrent que la fraude concerne tous les moyens de paiement, qu'il s'agisse du e-commerce ou du point de vente physique.

Face à cette réalité, un constat s'impose : la fraude ne disparaîtra pas. Mais elle peut être anticipée, contrôlée et transformée en un levier de fiabilité et de confiance.

Protéger son activité implique d'avoir de bons réflexes, de comprendre les comportements frauduleux, d'anticiper leurs évolutions et de déployer des défenses robustes, flexibles et intelligentes.

Ce livre blanc propose une analyse des principaux risques, des méthodes utilisées par les fraudeurs et des bonnes pratiques pour s'en prémunir. Parce qu'une brique paiement maîtrisée ne se contente pas de défendre : elle propulse la performance et devient un levier stratégique de croissance.



Données recueillies auprès de l'Observatoire de la sécurité des moyens de paiement (OSMP) en 2024

QU'EST-CE QUE LA FRAUDE AU MOYEN DE PAIEMENT ?

Définition

Cette fraude survient lorsqu'un **moyen de paiement** (carte, virement, prélèvement, chèque) est utilisé sans l'autorisation de son titulaire ou fait l'objet d'une contestation abusive. Dans les deux cas, le commerçant subit des préjudices et des conséquences directes : perte du montant de la commande, frais supplémentaires et surtout un climat de confiance avec ses clients fragilisé.

Comprendre les mécanismes de la fraude, c'est reprendre la maîtrise de sa brique paiement et transformer un risque en levier de fiabilité et de performance.

Fraude externe

Le titulaire de la carte ou du moyen de paiement **n'est pas à l'origine** de la transaction. Ses données bancaires ont été compromises (vol, phishing, piratage) et sont utilisées par une tierce personne pour réaliser un achat frauduleux. Le commerçant subit alors une perte immédiate avec la réception d'un impayé, difficilement contestable si la transaction n'a pas fait l'objet d'une authentification forte (type 3D Secure).

Friendly fraude

Plus insidieuse, la fraude amicale repose sur une **déclaration mensongère**. Le client **est bien à l'origine du paiement**, mais il le conteste volontairement auprès de sa banque. L'objectif est d'obtenir un remboursement abusif tout en conservant le bien ou le service.

On peut retrouver notamment la friendly fraude appliquée aux abonnements. Le porteur de carte valide le premier paiement (authentifié via 3D Secure), puis conteste les paiements suivants — appelés MIT (Merchant Initiated Transactions) — pour interrompre son abonnement sans passer par une procédure classique de résiliation.

Qu'elle soit externe ou «friendly», la fraude ne se limite pas à une commande perdue. Elle impacte :

- **La trésorerie**, par des flux financiers instables.
- **La productivité**, par le temps consacré à gérer les litiges.
- **La relation client**, par une confiance dégradée qui menace la fidélité.

L'ENJEU D'UN COMMERÇANT.

Le défi majeur d'un commerçant aujourd'hui est clair : **concilier croissance & sécurité.**

En d'autres termes, autoriser les transactions légitimes tout en limitant les fraudes qui diminuent ses marges.

Trois objectifs majeurs liés à des enjeux d'entreprise peuvent augmenter le risque de fraude.



Objectif

Enjeux

Parcours d'achat fluide

VS

Concurrentiels

Un parcours d'achat fragilisé.

Un processus trop contraignant fait perdre des clients au profit de concurrents qui offrent une expérience plus fluide.

Augmentation du chiffre d'affaires

VS

Financiers

Des transactions contestées.

Chaque chargeback entraîne le remboursement du montant initial, ainsi que des frais supplémentaires. Un impact immédiat sur les marges.

Fidélisation et acquisition de clients

VS

Image & réputation

Une confiance affaiblie.

Des incidents répétés altèrent la perception de fiabilité et dégradent la relation client sur le long terme.

La question n'est donc pas seulement de réduire la fraude. Il s'agit de s'approprier la brique paiement pour en faire un catalyseur de confiance et de performance. En maîtrisant les risques, le commerçant fluidifie ses parcours, protège ses marges et soutient une croissance durable.

QU'EST-CE QU'UN CHARGEBACK ?

Définition

Une transaction validée n'est pas toujours synonyme de paiement effectif. En e-commerce, une vente peut sembler aboutie... jusqu'à ce que le client conteste l'opération auprès de sa banque. Dans ce cas, les fonds déjà crédités sont retirés du compte du commerçant puis restitués à l'acheteur.

Il s'agit alors d'un impayé, également appelé **chargeback**.

À noter : un impayé est contestable en fonction de son motif avec des documents justificatifs. L'aboutissement en faveur du commerçant n'est cependant pas garanti.

Le chargeback/impayé peut être classé en 2 catégories.

Impayé fraude

L'acheteur conteste la transaction en affirmant ne pas en être à l'origine.

- Si la transaction a été authentifiée via 3D Secure avec transfert de responsabilité, le commerçant est protégé financièrement. Le risque est alors supporté par la banque de l'acheteur.
- Dans les autres cas, le commerçant reçoit un impayé, ce qui peut entraîner un coût direct et un impact immédiat sur la performance de son activité. Cependant, les impayés restent contestables et les fonds peuvent être récupérés selon les procédures mises en place.

Impayé service

L'acheteur conteste la transaction pour motif de litige commercial. Par exemple, il déclare ne pas avoir reçu le produit ou que le service livré ne correspond pas à la description initiale.

- Ce type d'impayé peut être contesté à l'aide de **preuves tangibles** (justificatifs de livraison, captures de commande, suivi logistique).
- La capacité du commerçant à **documenter** chaque étape de son processus devient alors un levier essentiel pour sécuriser ses revenus.

Les impacts d'un impayé

Un impayé ne se limite pas à une simple vente perdue. Il pèse sur la **rentabilité** d'une activité commerciale. Ses conséquences sont multiples :

- **Perte de chiffre d'affaires** sur le montant de la commande.
- **Frais supplémentaires** facturés par la banque.
- Temps de traitement administratif qui **ralentit** la productivité.
- Trésorerie **déstabilisée**.
- Confiance client et image de marque **dégradées**.

L'OBJECTIF DES FRAUDEURS.

La finalité d'une fraude liée à un moyen de paiement reste toujours la même pour le fraudeur : **l'obtention d'un bénéfice financier**. Cela se traduit par différentes stratégies :

➤ **Détourner des moyens de paiement légitimes** : collecte de données de paiement pour une réutilisation ou une revente.

➤ **Exploiter des données volées** : multiplication de transactions pour tester des données de paiement et générer un gain immédiat avant d'être détecté.

➤ **Convertir le bénéfice** : revente rapide des biens, demande de remboursement avec une autre méthode de paiement...



Des risques variables selon les moyens de paiement

Chaque moyen de paiement présente des niveaux de vulnérabilité distincts :

- **Risque financier direct** : paiements par carte sans transfert de responsabilité, prélèvements SEPA contestés...
- **Risque de fraude** : paiements par carte sans authentification forte par exemple.

Les techniques de fraude sont en constante évolution. C'est pourquoi la lutte contre la fraude ne peut pas se limiter à des outils techniques. Elle exige une **maîtrise** continue, une **vigilance** active et une capacité **d'anticipation** face aux scénarios d'attaque.

COMMENT SE PROTÉGER ?

La lutte contre la fraude ne repose pas sur une solution unique. Elle exige une **approche globale**, alliant maîtrise des risques, vigilance active, connaissance client et exploitation optimale des outils de prévention.

C'est cette combinaison qui transforme la protection en un levier durable de fiabilité et de performance.



Connaître les risques

La première étape pour renforcer la sécurité d'une activité consiste à **cartographier** ses vulnérabilités. Tous les moyens de paiement n'impliquent pas le même niveau de risque.

- **Les transactions sans authentification forte**, comme les paiements MOTO (Mail Order / Telephone Order), ou les saisies manuelles, figurent parmi les plus exposées.
- À l'inverse, un paiement par carte validé via **3D Secure** avec transfert de responsabilité, offre une meilleure protection au commerçant, puisque le risque est alors assumé par la banque de l'acheteur. Le transfert de responsabilité signifie que, lorsque l'authentification 3D Secure est réussie, c'est la banque de l'acheteur (et non plus le commerçant) qui prend en charge les pertes financières en cas de fraude.

Certaines situations requièrent également une vigilance renforcée :

- Commandes à **l'international** depuis des zones sensibles.
- Paniers **atypiques** ou montants exceptionnellement élevés.
- **Nouveaux** clients sans historique suffisant pour pouvoir analyser leur comportement.

Anticiper ces facteurs permet d'adopter une posture proactive plutôt que défensive, et d'optimiser les décisions de validation.

Connaître ses clients

Au-delà de l'analyse des moyens de paiement, la connaissance fine des comportements clients constitue un **pilier essentiel de la prévention**. Plus un commerçant connaît les habitudes de ses acheteurs, plus il lui est facile de repérer rapidement les anomalies.

Le fait qu'un client fidèle change soudainement de pays, d'adresse ou de panier moyen peut justifier un contrôle supplémentaire. À l'inverse, un nouveau client qui multiplie les tentatives de paiement ou demande une livraison hors de la zone géométrique définie par le commerçant représente un signal d'alerte à ne pas négliger.

Dans bien des cas, **un simple contact direct** (e-mail ou téléphone) suffit à lever les doutes. Cependant, si l'incertitude demeure, il est préférable de bloquer une commande suspecte plutôt que d'exposer son activité à un impayé lourd de conséquences.

Utiliser les outils à disposition

Les solutions de paiement intègrent aujourd'hui des **modules puissants et performants** de détection et de prévention de la fraude. Encore faut-il savoir les activer et les paramétrer de façon optimale.

Parmi les règles et outils qui peuvent être mis à disposition par un PSP comme Lyra :

- **Modules de sécurisation** : authentification forte 3D Secure, filtres anti-fraude, scoring dynamique.
- **Blocage géographique et IP** : refus automatique des transaction en provenance de certaines zones ou adresses IP suspectes.
- **Refus ciblés** : rejet des cartes prépayées ou à usage unique fréquemment utilisées par les fraudeurs.
- **Alertes intelligentes** : déclenchement d'une validation manuelle en cas de comportement suspect.

Un suivi **régulier** des chargebacks déjà rencontrés permet également d'ajuster et d'affiner les règles de filtrage, afin de renforcer la précision et l'efficacité du dispositif.

En cas de doute, le PSP peut accompagner le commerçant dans l'analyse des transactions sensibles et l'optimisation des paramètres de sécurité.

Être vigilant

La fraude évolue en permanence : les fraudeurs affinent leurs scénarios, exploitent de nouvelles failles et testent sans cesse les limites des systèmes. Pour rester compétitif, un commerçant doit instaurer une surveillance active et régulière de son activité.

Certains signes doivent attirer l'attention :

- Commandes **urgentes** ou demandes de livraison express atypiques.
- **Incohérences** entre adresses de facturation et de livraison.
- **Multiples** tentatives de paiement en série échouées.
- **Modifications** soudaines des informations (adresse, e-mail, numéro de téléphone).
- Connexions depuis une adresse IP **suspecte** ou incohérente avec le profil client.

La vigilance ne relève pas uniquement du **gestionnaire** : elle doit être partagée par l'ensemble des **collaborateurs**, du support à la logistique, afin de détecter et de remonter rapidement les comportements suspects.

Ces indices ne constituent pas toujours une fraude avérée, mais ils appellent à une vérification rapide. Tant que le produit n'a pas été expédié ou le service délivré, le commerçant conserve la maîtrise : **bloquer, rembourser ou annuler la transaction reste possible**.



Les scénarios de fraude à connaître



LE CARDING

“Le fraudeur essaie de payer en utilisant plusieurs cartes avec le même BIN (premiers chiffres de la carte).”

Définition

Le carding est une fraude en e-commerce consistant à tester massivement des numéros de cartes bancaires volées ou contrefaites afin d'identifier celles encore actives. Les fraudeurs utilisent des bots ou scripts automatisés qui envoient en quelques minutes des centaines de tentatives. Souvent, ces essais proviennent du même BIN et reposent sur des données issues de phishing, malwares ou bases revendues sur des forums clandestins.

Même sans achat réel, le carding engendre des impacts techniques (saturation du serveur de paiement, ralentissements, blocages), financiers (multiplication des frais d'autorisation), et réputationnels (perte de confiance des clients et partenaires). Les cartes validées servent ensuite à d'autres fraudes chez d'autres commerçants.

Repérer le carding

Plusieurs indicateurs peuvent alerter le commerçant sur une activité suspecte :

- Une **même adresse e-mail ou IP** tente de nombreuses transactions avec des cartes différentes.
- Des **BINs ou dates d'expiration** identiques sur plusieurs tentatives.
- Des **échecs** répétés suivis d'un ou deux paiements validés.
- Des commandes passées à des horaires **inhabituels**, parfois la nuit.
- Une forte activité en provenance de **zones géographiques peu habituelles**.

Le carding n'est jamais invisible.

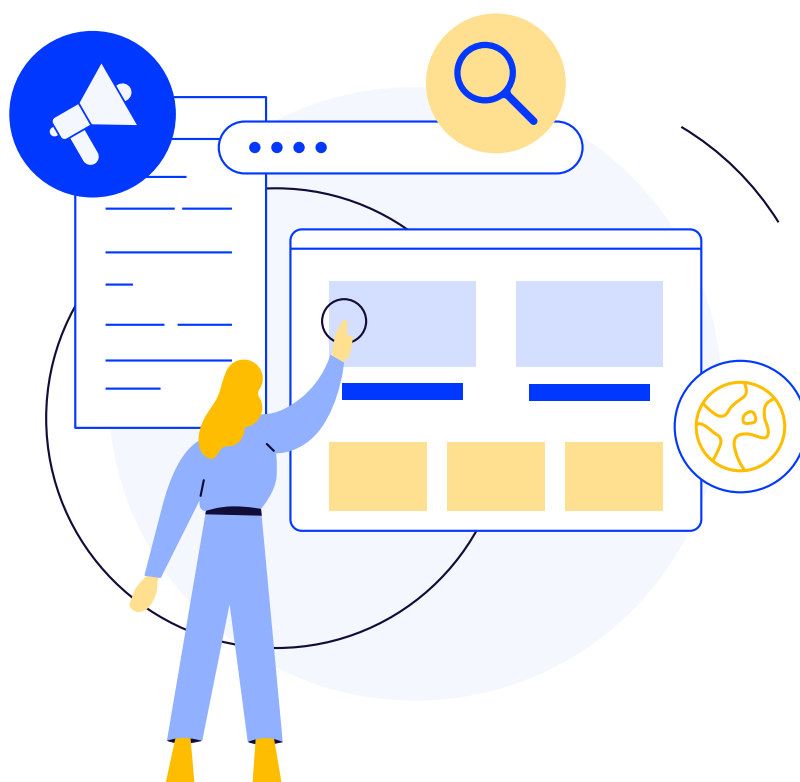
Avec des outils de suivi adaptés, il est possible de le détecter rapidement.

Comment se protéger ?

Pour contrer le carding, il ne suffit pas de réagir après coup : l'approche doit être préventive et proactive. Parmi les bonnes pratiques essentielles :

- Mettre en place **des règles de vélocité**, par exemple bloquer une adresse e-mail qui utilise plus de 3 cartes en 5 minutes.
- Utiliser des outils et **des filtres intelligents** mis à disposition par le PSP : scoring dynamique, surveillance en temps réel, alertes automatisées.
- Déployer des **CAPTCHA** (Completely Automated Public Turing test to tell Computers and Humans Apart), tests permettant de différencier un humain d'un robot, afin de freiner les scripts automatisés.
- **Surveiller** les tentatives de paiement échouées, souvent signes avant-coureurs d'un carding.
- **Bloquer** ou annuler les transactions suspectes avant expédition, même si le paiement semble validé.

En renforçant sa vigilance et en exploitant pleinement les outils de prévention, un commerçant peut neutraliser le carding avant qu'il n'impacte sa performance et ne compromette la fiabilité de son site.



ABUS DE CONFIANCE

MOTO

“Le fraudeur demande à réaliser un paiement à distance via une saisie manuelle des données de la carte par le commerçant (MOTO : Mail Order Telephone Order).”

Définition

Le MOTO (Mail Order Telephone Order) désigne une transaction saisie manuellement par le commerçant soit sur un TPE physique en in-store, soit via un formulaire de paiement en e-commerce, sans authentification forte. Cette pratique, encore utilisée dans certains secteurs d'activité pour répondre à des demandes à distance, représente une vulnérabilité majeure. Les fraudeurs exploitent ce canal peu sécurisé en appelant directement le commerçant, souvent sous prétexte d'urgence ou de situation exceptionnelle, ils se servent de numéros de cartes bancaires volées.

La transaction est validée, le produit est livré mais quelques jours plus tard, le véritable titulaire de la carte conteste l'opération. Résultat : le commerçant subit un impayé et supporte seul la perte financière.

Mode opératoire

Commerçant (Victime)

Il reçoit une commande par téléphone, en ligne ou par e-mail.

La commande paraît alléchante, ce qui l'incite à l'accepter.

Le commerçant saisit manuellement les cartes utilisées par le fraudeur.

Une fois la transaction validée, il expédie la commande.

Quelques jours plus tard, il reçoit des impayés non contestables liés aux cartes utilisées.

Client (Fraudeur)

Il se présente comme un client pressé, incapable de se déplacer et exige une livraison rapide.

Il transmet plusieurs numéros de cartes jusqu'à ce que l'un d'eux fonctionne.

Il demande rapidement confirmation de la livraison.

Il mandate quelqu'un pour récupérer le colis dans un délai très court.

Il disparaît avec la commande avec l'objectif de la revendre et reste injoignable.

1

2

3

4

5

Comment se protéger ?

- Redoubler de vigilance sur les **produits à forte valeur** de revente.
- Se méfier des commandes atypiques ou anormalement élevées, surtout avec une **livraison urgente**.
- Demander une pièce d'identité ou **une preuve** de titularité de la carte avant d'accepter la transaction.
- Sensibiliser les équipes pour leur **apprendre à dire non**, même en cas de pression.
- Limiter au maximum l'usage du MOTO et privilégier un paiement avec authentification forte, par exemple via un lien de **paiement sécurisé**.



ABUS DE CONFIANCE - GOLD DIGGER

“Le fraudeur est très intéressé par ce que je vends, car il pourra le revendre facilement.”

Définition

La fraude par abus de confiance vise particulièrement les commerçants qui vendent des produits à **forte valeur** et **facilement revendables** comme les smartphones, l'électronique ou les pièces mécaniques. Le fraudeur se présente comme un client légitime. Il passe commande, insiste sur une livraison urgente, puis récupère le produit pour le revendre rapidement. Quelques jours plus tard, le véritable titulaire de la carte conteste le paiement.

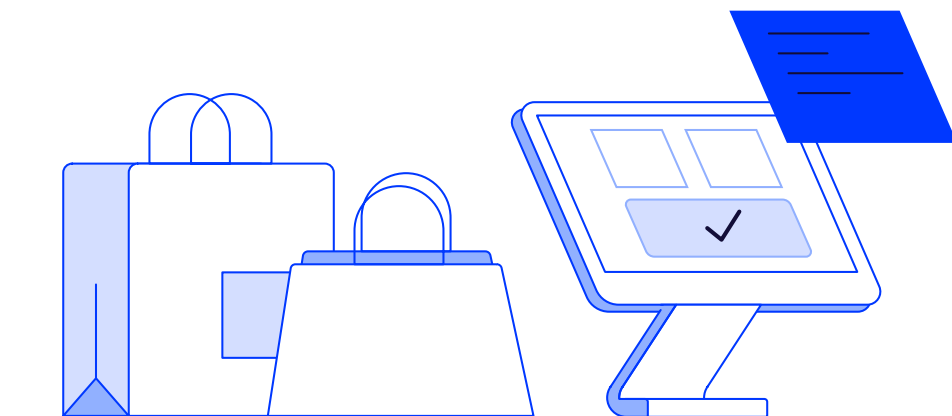
Pour maximiser ses gains, le fraudeur **multiplie** les tentatives avec différentes cartes, souvent issues de pays variés et utilise une même adresse, parfois celles de complices. Dans ce scénario, le commerçant supporte seul la perte financière.

Repérer le gold digger

Certains indices permettent de détecter ce type de fraude :

- Une **même adresse e-mail** teste plusieurs cartes en très peu de temps, souvent depuis des zones géographiques différentes.
- Plusieurs comptes ou acheteurs distincts utilisent la **même adresse de livraison**.
- Après la commande, le client contacte le service pour **accélérer la livraison**, insistant fortement sur l'urgence.

Attention : un fraudeur expérimenté sait paraître coopératif et rassurant. Contacter directement le client ne suffit donc pas toujours à identifier la fraude.



Comment se protéger ?

Contrôler la vitesse et les zones à risques :

- **Bloquer** ou alerter lorsqu'une même adresse e-mail teste plusieurs cartes en quelques minutes.
- **Filtrer** par zone géographique : si la clientèle est majoritairement locale, restreindre certaines zones à risques ou hors Europe.
- **Vérifier** les adresses de livraison : une même adresse utilisée par plusieurs comptes doit déclencher une alerte, sauf dans le cas de points relais connus.

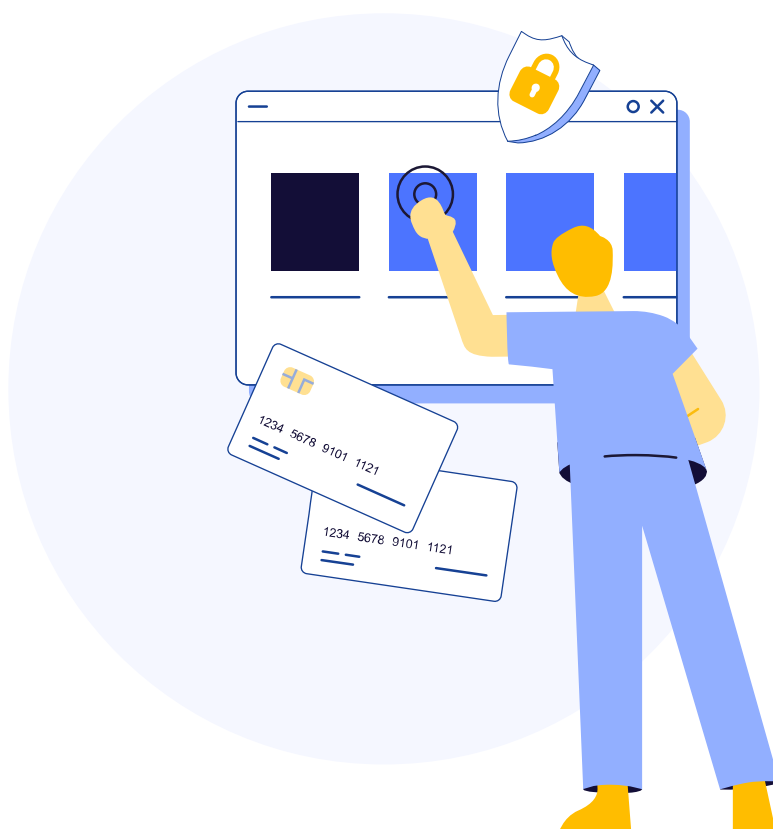
Former les équipes :

- **Sensibiliser** le service client aux commandes à risque : toute demande pressante doit éveiller la vigilance.
- **Encourager** la prudence : retarder ou bloquer une expédition en cas de doute vaut mieux que subir une perte sèche.
- **Documenter** chaque interaction suspecte pour créer un historique utile en cas de litige.

Combiner vigilance humaine et outils automatiques :

Même bien déguisées, ces tentatives peuvent être contrées grâce à une combinaison de règles simples et de vigilance humaine.

Les filtres et systèmes de détection ne repèrent pas toujours l'ensemble des signaux. Un contrôle manuel ciblé sur les commandes à forte valeur, ou présentant plusieurs critères de risques, renforce la détection et préserve les ventes.



LE CAMOUFLAGE

“Le fraudeur essaye de se faire passer pour un client normal.”

Définition

Le camouflage est l'une des formes de fraude les plus insidieuses pour les commerçants. Contrairement aux attaques massives ou voyantes, le fraudeur mise sur **la discrétion**.

Son objectif : imiter en tout point un client légitime afin d'effectuer une transaction frauduleuse sans éveiller le moindre soupçon.

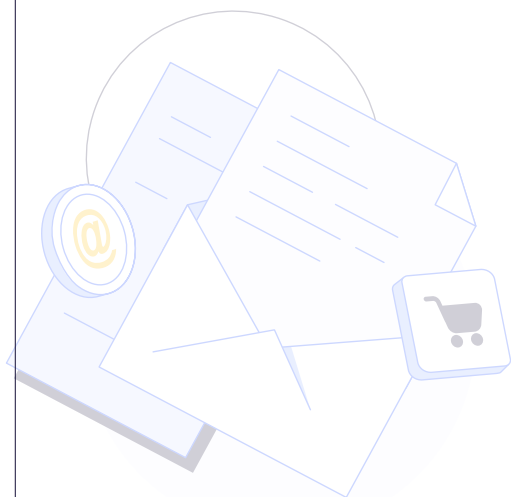
Ce scénario est particulièrement redoutable car si le fraudeur attire l'attention, il est immédiatement bloqué. Il **s'adapte** donc en jouant sur les détails : comportement d'achat réaliste, montants plausibles, informations crédibles. Le commerçant découvre la fraude trop tard, le plus souvent au moment du chargeback, une fois la commande expédiée et les pertes irréversibles.

Repérer le camouflage

Identifier un fraudeur camouflé est complexe, c'est l'une des formes de fraude les plus difficiles à détecter en temps réel. Pourtant, certains signaux peuvent alerter :

- Transactions **inhabituables** : plusieurs petites commandes passées en peu de temps avec la même carte ou le même e-mail.
- Adresses **suspectes** : une même adresse de livraison utilisée par différents acheteurs.
- Identités **douteuses** : noms intégralement en minuscules, formulations étranges, jeux de mots suspects ou encore usurpation de célébrités comme client.
- **Réclamations fréquentes** : contestations d'achats répétées ou retours multiples pour des motifs discutables.

À noter : un signal isolé ne suffit pas toujours à détecter un fraudeur camouflé. En revanche, l'observation d'un schéma récurrent dans le temps permet souvent de révéler ces comportements discrets et de protéger l'activité.



Comment se protéger ?

Pour contrer le camouflage, il est essentiel de combiner règles automatiques, vigilance humaine et analyse continue des données passées.

Mettre en place des règles réactives

- **Bloquer** les e-mails suspects : toute adresse déjà utilisée pour fraude doit être automatiquement exclue.
- **Surveiller** les adresses de livraison utilisées par plusieurs comptes et déclencher une alerte ou un blocage en cas de suspicion.
- **Règles de vélocité** : plusieurs transactions rapprochées avec la même carte ou le même e-mail doivent être signalées.

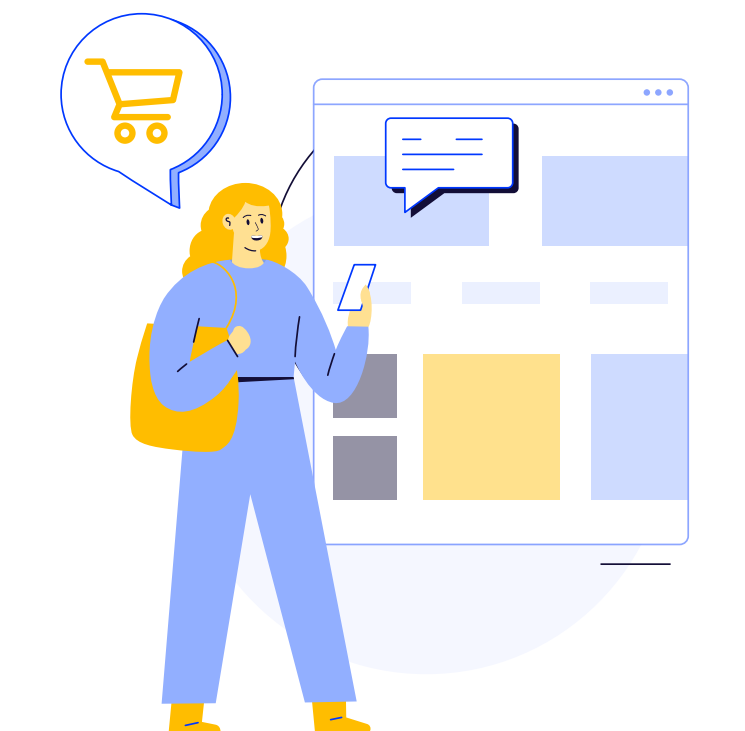
Sensibiliser les équipes

- Former les équipes à repérer ces signaux faibles renforce considérablement la protection.

Conserver et analyser les données pour enrichir les règles de protection

- Chaque fraude passée est une opportunité d'apprentissage. L'étude des chargebacks et des transactions frauduleuses permet d'améliorer les règles existantes, d'affiner les alertes et de réduire les opportunités laissées aux fraudeurs.

En résumé, face au camouflage, **l'adaptation continue** est la clé : plus le commerçant maîtrise et enrichit ses règles au fil de ses expériences, plus il renforce la fiabilité de ses paiements et protège durablement sa performance.



LE MIRAGE

« La commande est trop belle pour être vraie »

Définition

Le mirage est une fraude subtile qui joue sur l'émotion et l'urgence. Le fraudeur cherche à susciter l'enthousiasme ou à instaurer un sentiment de pression pour pousser le commerçant à l'aider coûte que coûte. Sous cette influence, le commerçant peut perdre en vigilance, ignorer certains signaux d'alerte et valider une transaction risquée. L'objectif est clair : obtenir l'autorisation d'une transaction coûteuse avant que le risque ne soit identifié.

Repérer le mirage

Le mirage se détecte à travers une combinaison de comportements insistants et inhabituels :

- > **Montants atypiques** : une commande particulièrement élevée ou disproportionnée.
- > **Moyens de paiement douteux** : insistance pour un paiement sans authentification forte, comme le paiement MOTO par exemple, souvent justifiée par une situation exceptionnelle.
- > **Urgence excessive** : pression pour traiter la transaction immédiatement, exploitant le stress ou l'empressement du commerçant.
- > **Excuses répétitives** : plusieurs cartes testées (conjoint, parent, voisin...), tant que le commerçant reste coopératif.

Pris isolément, ces signaux peuvent sembler anodins. Mais leur accumulation dessine un scénario typique du mirage.



Comment se protéger ?

Signaler et bloquer ce comportement

Toute situation qui déclenche plusieurs alertes (montant inhabituel, paiement MOTO, pression liée à l'urgence) doit immédiatement être signalée et évaluée par les équipes responsables de la sécurité.

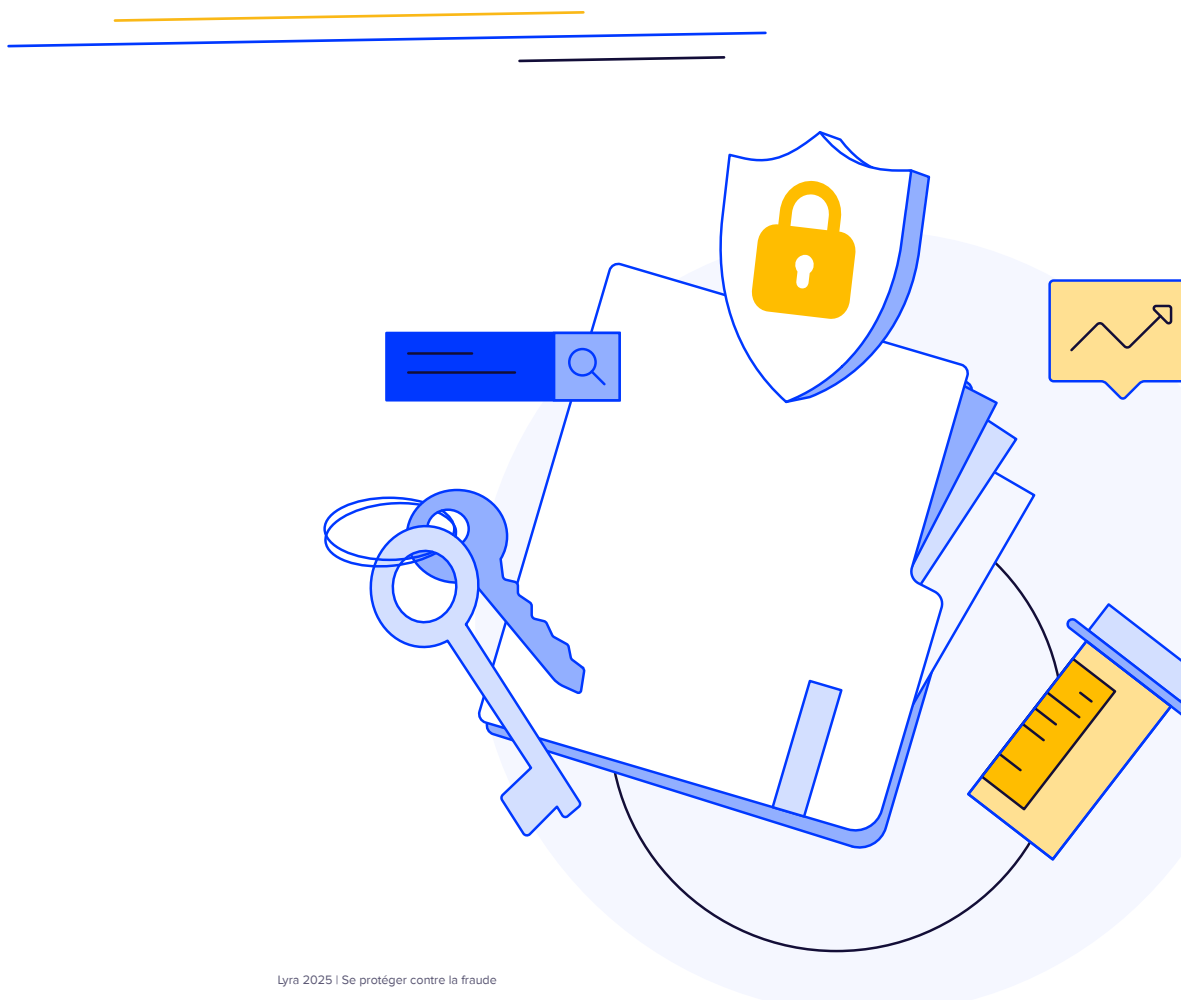
Sensibiliser les équipes

La vigilance humaine est cruciale, il faut faire appel au bon sens. La règle d'or : si c'est trop beau pour être vrai, c'est que ça ne l'est pas toujours. Les équipes doivent savoir reconnaître les schémas typiques du mirage et résister à la pression du client.

Mettre fin à la transaction à risque

Ne jamais laisser le scénario se poursuivre. Un fraudeur persistant ne s'arrêtera que lorsque la transaction est refusée. Les tentatives répétées avec différentes cartes ou excuses doivent entraîner une suspension immédiate de la commande.

En résumé, le mirage exploite la psychologie du commerçant : enthousiasme, empathie et urgence sont ses leviers. La prévention repose sur la vigilance, la connaissance des signaux faibles et la fermeté face aux comportements suspects. En agissant rapidement et avec discernement, le commerçant protège ses ventes, sa rentabilité et sa fiabilité.



L'INGÉNIERIE SOCIALE

“Le fraudeur appelle en se faisant passer pour un collègue ou un partenaire de confiance afin d’obtenir des informations sensibles.”

Définition

Si la fraude s’appuie souvent sur la technologie, elle passe aussi par une arme plus subtile : **la manipulation humaine**. L’ingénierie sociale consiste à amener un collaborateur ou un commerçant à révéler, parfois sans s’en rendre compte, des informations sensibles ou à effectuer une action compromettante. Ici, ce n’est pas la technique qui cède, mais la vigilance humaine.

Ce type de fraude représentait **382 millions d’euros** en 2024 (source OSMP)

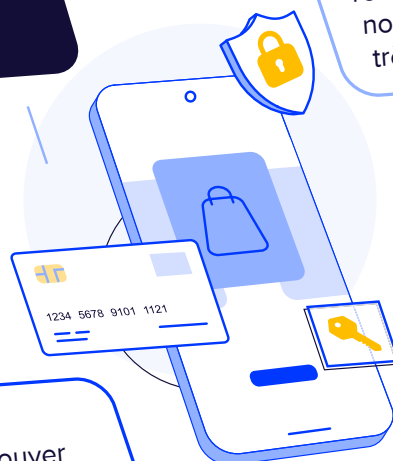
Les fraudeurs exploitent **la confiance, l’urgence ou la crédulité** pour déverrouiller l’accès à des données critiques. Leur objectif est clair : contourner les protections techniques en manipulant directement ceux qui les utilisent. Avec la montée en puissance de l’IA (imitations de voix, deepfakes, redirection de lignes téléphoniques), ces attaques deviennent plus sophistiquées, plus crédibles et donc plus dangereuses.

“ Bonjour, ici le support de votre prestataire de paiement. Nous devons vérifier en urgence vos accès au back-office pour éviter le blocage de vos encaissements. Pourriez-vous me transmettre vos identifiants ? ”

“ Bonjour, j’ai passé commande hier mais je me suis trompé de montant. Pourriez-vous me rembourser rapidement sur ce nouveau compte bancaire, c’est très urgent. ”

“ Bonjour,
Nous vous prions de trouver ci-dessous nos nouvelles coordonnées bancaires. Merci de l’enregistrer et de l’utiliser pour le règlement de vos futurs achats. ”
-Votre fournisseur.

“ Vous avez un nouveau message. Pour l’écouter, veuillez cliquer ici. ”



Repérer l'ingénierie sociale

PRETEXTING

Le fraudeur invente un scénario crédible (problème urgent, demande client fictive, autorité hiérarchique simulée) pour inciter à divulguer des informations confidentielles.

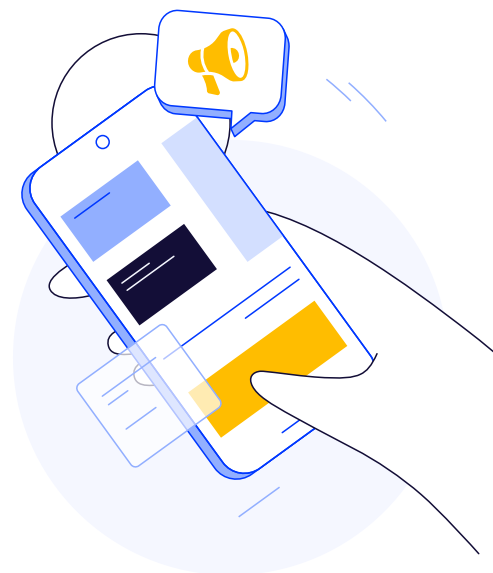
IMPERSONATING

Le fraudeur se fait passer pour quelqu'un de confiance afin d'obtenir une action compromettante.

ex : virement urgent sans justificatif

PHISHING

Un e-mail ou SMS imitant une source légitime incite la victime à cliquer sur un lien frauduleux et à saisir ses données sur un site web falsifié.



Comment se protéger ?

La lutte contre l'ingénierie sociale repose moins sur des outils que sur **une culture de sécurité partagée**. Chaque collaborateur doit devenir un acteur de fiabilité.

Quelques bonnes pratiques clés :

- Ne jamais divulguer **d'informations sensibles** dans la précipitation : tout ce qui paraît urgent mérite d'être vérifié.
- **Limiter la diffusion de données personnelles ou professionnelles** : même une information anodine (adresse e-mail, date de vacances, nom d'un proche) peut être exploitée.
- Toujours **vérifier la légitimité** d'un interlocuteur : un contre-appel ou une validation via un canal officiel réduit considérablement les risques.
- **Anonymiser ou chiffrer les données sensibles** lorsque cela est possible, afin de limiter leur exploitation.
- **Former** régulièrement les équipes : comprendre les méthodes des fraudeurs permet de mieux les anticiper et d'y résister.

PRISE DE CONTRÔLE.

« Un hacker détourne mon site à l'étape du paiement »

Définition

La prise de contrôle se produit lorsqu'un fraudeur parvient à pirater le site d'un commerçant. À l'étape du paiement, il détourne les fonds vers son propre compte ou redirige les clients vers une page de paiement fictive afin de capter leurs données bancaires.

L'attaque est ciblée et ses effets sont immédiats : chaque transaction validée disparaît avant d'atteindre le compte du commerçant. Le risque est critique, car la fraude n'est souvent détectée qu'au moment de constater l'absence de commandes abouties, ou pire, de réception des fonds.

Repérer la prise de contrôle

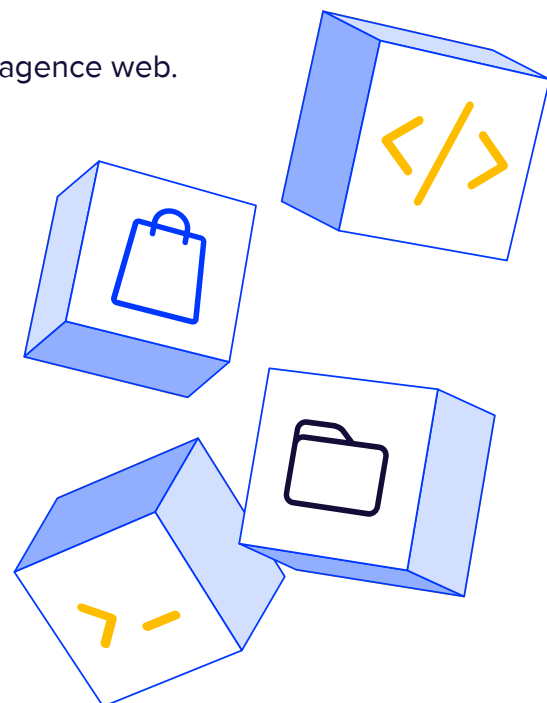
Le signe le plus évident est l'**absence de fonds encaissés**, malgré des transactions validées. Mais d'autres indices doivent aussi éveiller la vigilance :

- **Redirections inhabituelles** vers des pages externes ou non reconnues.
- **Modifications** non prévues sur le site, même mineures.
- **Alertes de sécurité émises** par l'hébergeur, le CMS ou l'agence web.

Comment se protéger ?

Face à une prise de contrôle, la rapidité d'action est essentielle :

- **Suspendre temporairement l'activité du site** : stopper les ventes empêche toute nouvelle perte et protège les clients le temps de rétablir la situation.
- **Sécuriser et reprendre le contrôle** : après analyse de l'intrusion, appliquer les règles de sécurité (mise à jour des mots de passe ou du plugin) et restaurer le code ou les paramètres. Si besoin, faire appel à son prestataire de paiement pour contrôler le bon fonctionnement avant de relancer l'activité.
- **Renforcer la sécurité du site sur le long terme** : activer une authentification renforcée, déployer un monitoring en continu et configurer des alertes en temps réel pour repérer toute anomalie avant qu'elle ne devienne critique.



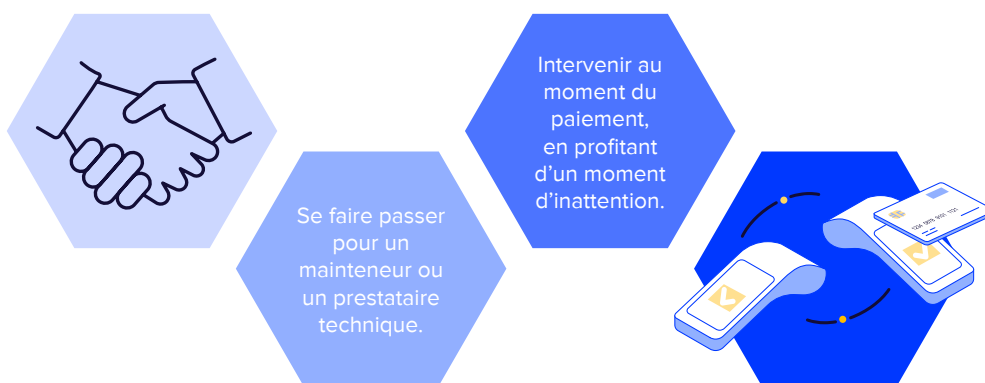
ÉCHANGE DE TERMINAL DE PAIEMENT

« Le fraudeur vient dans ma boutique pour subtiliser mon TPE »

Définition

L'échange de terminal survient lorsqu'un fraudeur **prend le contrôle du point d'encaissement physique**. Il détourne l'attention du commerçant pour remplacer le TPE légitime par un **terminal pirate**. Les fonds encaissés sont alors redirigés vers un compte tiers, que le fraudeur peut récupérer facilement. Cette méthode peut également cibler les QR codes statiques affichés en point de vente, qui sont manipulés pour détourner les paiements.

Mode opératoire



Repérer l'échange de TPE

Le premier indice reste évident : **les fonds n'arrivent plus**. Mais d'autres signaux peuvent alerter, comme l'absence de visibilité des paiements dans le back office, des incohérences entre les montants validés et les sommes réellement encaissées, des messages inhabituels sur le terminal, une apparence modifiée du TPE ou encore des informations erronées sur les tickets.

Comment se protéger ?

- **Surveiller le terminal** : ne jamais laisser un TPE sans surveillance, qu'il s'agisse des heures d'ouverture ou de fermeture. Vérifier systématiquement son intégrité avant utilisation et repérer tout signe d'altération.
- **Agir rapidement** : au moindre doute ou en cas de manipulation suspecte, isoler et remplacer immédiatement le terminal concerné.
- **Renforcer la vigilance collective** : former les équipes à reconnaître les tentatives d'usurpation et à vérifier l'identité des intervenants techniques.
- **Sécuriser les contrôles quotidiens** : comparer les montants, identifiants commerçant et codes banque sur les tickets et télécollectes, et vérifier l'authenticité des QR codes utilisés.

LA FRAUDE PAR FACTURE CRÉDIT

« Le fraudeur fait des remboursements sur ses cartes depuis un TPE pirate en puisant dans mes comptes »

Définition

La fraude à la facture crédit consiste pour un fraudeur à détourner le mécanisme de remboursement. À l'aide d'un TPE pirate, il crédite des cartes prépayées qu'il contrôle directement depuis le compte du commerçant. Les fonds sont ensuite retirés ou transférés en un instant, laissant le commerçant face à une perte irréversible et sans recours possible.

Repérer la fraude par facture crédit

La détection repose sur une surveillance fine des flux financiers. Quelques signaux doivent immédiatement alerter :

- **Remboursements non autorisés** : toute opération qui n'a pas été initiée par les équipes internes doit être traitée comme critique.
- **Schémas répétitifs** : mêmes montants, mêmes cartes, ou une série de remboursements concentrés en quelques minutes.
- **Flux inhabituels** : remboursements à des horaires atypiques, sur des cartes rarement utilisées, ou avec un volume supérieur à la normale.
- **Écarts comptables** : comparer régulièrement les reçus TPE aux relevés bancaires permet de repérer rapidement une anomalie.

Ces indices, même minimes, constituent des signaux faibles précieux pour anticiper et stopper une fraude avant qu'elle ne compromette la rentabilité.

Comment se protéger ?

La protection contre la fraude à la facture crédit repose sur une combinaison de maîtrise opérationnelle et de réactivité immédiate :

- **Contrôler les flux quotidiennement** : vérifier systématiquement les remboursements et les rapprocher des ventes réelles pour détecter tout écart.
- **Réagir sans délai** : au moindre doute, bloquer le TPE suspect et engager une investigation avant que d'autres opérations ne soient initiées.
- **Mettre en place des alertes automatiques** : déclencher une notification dès qu'un remboursement inhabituel apparaît (montant identique répété, fréquence accélérée, volume anormal).
- **Renforcer la gestion des accès** : limiter les droits aux seuls collaborateurs autorisés à paramétrer ou valider un remboursement.
- **Capitaliser sur l'expérience** : documenter chaque tentative de fraude afin d'améliorer les procédures internes et renforcer la formation des équipes.

Vous souhaitez en savoir plus ou mettre en place une stratégie de lutte contre la fraude adaptée à votre activité ?

Nos experts en surveillance des transactions sont à votre disposition pour analyser vos besoins, vous conseiller sur les meilleures pratiques et vous accompagner dans le déploiement de solutions efficaces.

CONTACTEZ NOS EXPERTS

Ensemble, faisons de votre brique paiement un levier stratégique contre la fraude.
