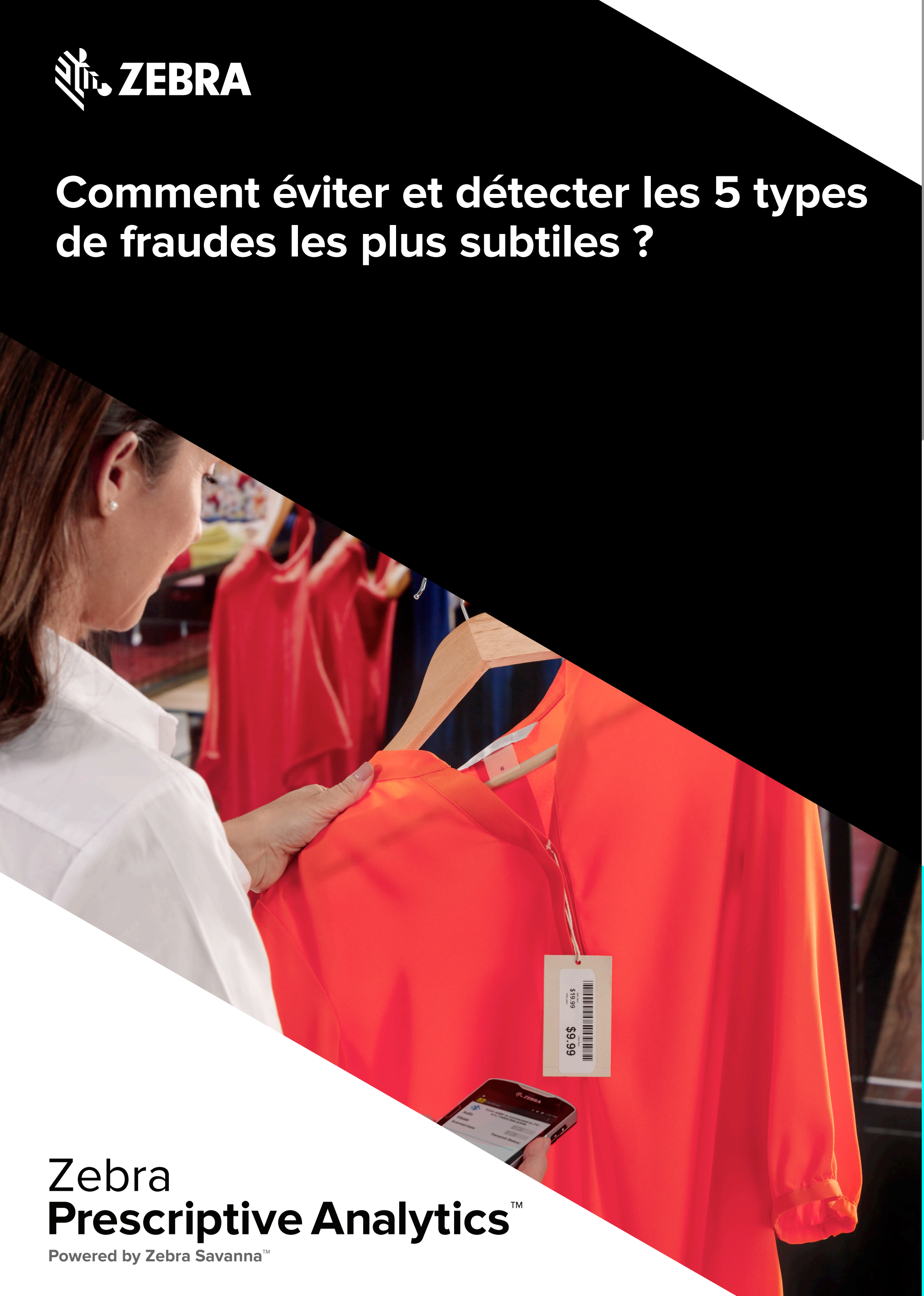
Comment éviter et détecter les 5 types de fraudes les plus subtiles ?



Zebra
Prescriptive Analytics™

Powered by Zebra Savanna™

Dans cet e-book, vous apprendrez à :

- Connaître cinq types de fraudes internes
- Suivre les données qui éveillent les soupçons
- Identifier et éliminer les risques à l’aide d’analyses avancées

Introduction

Pas question de plaisanter avec la fraude alors que la concurrence fait rage dans le secteur du commerce et de la distribution. Les marges fondant comme neige au soleil du fait d'une guerre des prix sans merci, les enseignes doivent sévir contre la fraude, à plus forte raison lorsqu'elle est commise par leurs propres collaborateurs. Non seulement les employés connaissent parfaitement les mécanismes de sécurité des enseignes (et savent, par extension comment les contourner), mais ils ont aussi accès à des fonctions de caisse hasardeuses et à des marchandises non protégées dans les arrière-boutiques, les entrepôts et les camions. Cette connaissance d'initiés rend difficile la détection des fraudes internes, malgré la mise en place de caméras de surveillance et d'autres mesures de sécurité.

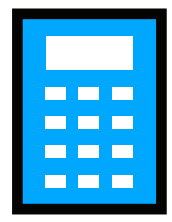
Face à ce défi, de nombreuses enseignes exploitent leurs données pour identifier toute activité suspecte de la part de leurs employés. Elles savent qu'il est impossible de manipuler les données et qu'une solution d'analyse adaptée, comme l'analyse prescriptive, peut mettre au jour des comportements spécifiques laissant supposer une fraude ou d'autres activités malveillantes susceptibles d'éroder les marges. Cet ebook présente cinq exemples extrêmement subtils de fraude commise par les employés, ainsi que les comportements de données révélateurs que l'analyse prescriptive peut identifier.


ZEBRA

Cinq types de fraudes internes extrêmement subtils

1. Coulage caisse

2. Usage illicite d'un code PIN de manager

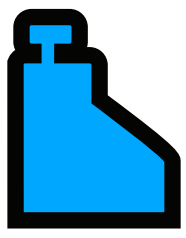


3. Détournement de cartes de fidélité

4. Échange d'étiquette et complaisance

5. Fraude du service client de l'e-commerce

Fraude n° 1



Coulage caisse

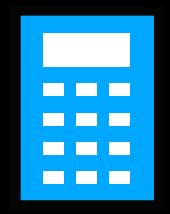
On parle de « coulage » lorsqu'un personnel en caisse passe un article devant un scanner en masquant délibérément le code-barres. Le client (généralement un complice) est alors libre d'emballer l'article et de quitter le magasin sans l'avoir payé. Les vidéos de surveillance ou la surveillance physique ne suffisent pas à qualifier cette activité de fraude. Vous aurez beau confirmer l'omission d'un article, vous aurez du mal à prouver qu'il s'agit d'une action délibérée et non d'une simple erreur naïve.

Les données peuvent néanmoins vous aider. Pour identifier le coulage caisse, vous pouvez analyser les taux de lecture par minute ou par heure de chaque caissier/caissière. Ce processus exige une bonne solution analytique, comme l'analyse prescriptive, à même de « clustériser » (regrouper

en fonction de caractéristiques similaires) le personnel de caisse et les magasins de façon à faire ressortir des moyennes de référence pour certains KPI, comme les taux de lecture. Tout personnel de caisse dont le taux de lecture se situe à trois écarts types en dessous du chiffre de référence peut être considéré comme fraudeur potentiel.

Surtout si ces taux suspects sont constatés sur des périodes « à haut risque » (heures du déjeuner, heures de pointe, pause ou absence du superviseur, etc.). L'analyse prescriptive tient compte de ces circonstances pour identifier les fraudes potentielles.

Fraude n° 2



Usage illicite d’un code PIN de manager

Pour éviter tout risque en cas d’annulation, d’erreur de prix et autres activités de ce type, les enseignes demandent souvent aux superviseurs de saisir un code d’identification personnel (PIN) pour obtenir l’autorisation voulue. Il est malheureusement très facile de détourner un code PIN. Le personnel de caisse peut l’avoir mémorisé ou le manager peut l’avoir partagé pour gagner du temps. Ce comportement doit absolument cesser, au risque de voir un seul hôte de caisse voler des milliers d’euros en espèces ou en marchandises.

Les données, notamment les données des ressources humaines, offrent plusieurs moyens d’identifier une fraude au code PIN. Les solutions analytiques les plus abouties intègrent des données issues de plusieurs applications ou fournisseurs. Vous pouvez ainsi visualiser facilement ces jeux de données distincts et en tirer des informations dans une seule et unique interface.

Pour détecter l’usage illicite d’un code PIN de manager, vous pouvez déployer un « modèle » (un algorithme chargé de rechercher des comportements de données spécifiques) qui compare, par analyse croisée, chaque code PIN aux données de la paie. Ce modèle vous alerte chaque fois qu’un code PIN de manager est utilisé alors que son propriétaire n’est pas censé travailler.

Si vos managers utilisent des terminaux mobiles dotés de services de géolocalisation, une solution analytique peut également vérifier la distance qui sépare le manager de la caisse au moment de la saisie du code PIN. Si le superviseur se trouvait à l’autre bout du magasin à cet instant précis, le responsable de la protection des actifs est immédiatement prévenu.

Fraude n° 3

Détournement de cartes de fidélité

La plupart des enseignes autorisent les clients à saisir un numéro de téléphone en caisse pour consulter leurs comptes de fidélité. Il arrive que le personnel de caisse exploite ce service à leur profit en entrant leur propre numéro de téléphone à la place de celui du client, raflant au passage leurs primes de fidélité. Ce comportement passe souvent inaperçu à moins que le client ne suive de près son nombre de points.

Les fonctions de comparaison et de clustérisation des outils analytiques sophistiqués dont nous avons parlé permettent de faire ressortir de vos données les preuves d'une fraude aux programmes de fidélité. Ces solutions recherchent un excédent de points sur les comptes de fidélité de vos collaborateurs. Un compte d'employé dont le nombre de points augmente tout d'un coup à un rythme supérieur à la moyenne nécessite une étude plus approfondie.

Les employés peuvent également usurper les numéros de téléphone associés à des comptes présentant un nombre élevé de points et s’en servir pour acheter de la marchandise ou du carburant à prix très réduit.

Comme dans l’exemple précédent, la solution adaptée peut être configurée de manière à repérer les comptes affichant une hausse inexpliquée des dépenses, surtout si les achats concernent des cibles privilégiées comme les produits électroniques, le carburant ou les cartes cadeaux. Peut-être victimes de piratage, ces comptes doivent faire l’objet d’une enquête.

Fraude n° 4

Échange d’étiquette et complaisance

Il s’agit là de la technique favorite des réseaux de fraude organisée. Elle implique souvent des employés de rayons qui vendent des articles au poids, comme le rayon Boucherie. Puisqu’ils impriment les étiquettes de prix sur place, ils n’ont aucun mal à apposer des étiquettes d’articles moins chers sur des produits de haute qualité (étiqueter des morceaux de bœuf très prisés comme entrecôte ou tournedos, normalement à 34€ le kilo, au prix de cuisses de poulet à 9€ le kilo).

Il existe une technique similaire, dite de « complaisance », où un caissier utilise un code de référence d’un article bon marché (un chewing gum à 25 centimes) pour encaisser le produit beaucoup plus cher de son complice (un parfum haut de gamme à 89 euros).

Vous parviendrez sûrement à détecter ces comportements suspects dans un rapport d’inventaire, mais vous aurez bien du mal à distinguer une fraude d’une simple variation de la demande.

Pour identifier ces échanges de prix, il suffit souvent de surveiller vos mouvements de stock. Toutes ces fausses ventes se traduisent par des mouvements de stock anormalement élevés pour les produits moins chers et anormalement faibles pour les produits volés. Ces deux comportements sont la preuve manifeste d’une fraude au prix, surtout s’ils ne se produisent que dans quelques magasins.

Une solution analytique avancée détecte facilement des anomalies de cette nature. Elle fait non seulement ressortir ces modèles de vente, mais identifie aussi la caisse ayant encaissé le plus d’articles de faible prix. Elle extrait ensuite les séquences vidéo correspondant aux heures des passages en caisse, vous permettant ainsi de voir exactement ce qui a été encaissé et pour quel montant. Votre enquête avance beaucoup plus vite et vous pouvez intervenir plus rapidement et avec plus de précision.

Fraude n° 5

Fraude du service client de l’e-commerce

C’est une réalité de l’e-commerce : des colis peuvent disparaître au cours du transport et ne jamais arriver chez le client. La plupart des enseignes remplacent gratuitement les produits perdus. Certaines envoient une carte cadeau ou un avoir sur le prochain achat pour dédommager les clients.

Cette pratique donne aux agents du service client une occasion en or de frauder. Des enseignes ont découvert que certains d’entre eux faisaient livrer ces commandes de remplacement chez eux ou chez des comparses, quelquefois dans le cadre d’un réseau de fraude organisée beaucoup plus vaste. Ces incidents représentant rapidement des pertes de plusieurs milliers d’euros, il est essentiel de les identifier et d’y mettre un terme au plus vite.

De nombreux fils de données peuvent éveiller les soupçons avant même que des pertes soient constatées. Voici quelques exemples :

- **Destinations des remplacements.** Les commandes de remplacement expédiées aux alentours d'un centre d'appel ont toutes les chances d'être frauduleuses. Si plusieurs commandes de remplacement sont expédiées à un même petit groupe d'adresses, elles doivent immédiatement faire l'objet d'une enquête, surtout si les adresses correspondent aux coordonnées des employés. L'analyse prescriptive identifie ces anomalies et vous prévient tout de suite.

- **Fréquence des remplacements.** Comme nous l'avons déjà dit, les solutions analytiques avancées peuvent calculer des moyennes de référence pour des comportements comme le remplacement de commandes. En comparant les moyennes de tous les agents à celle des taux de remplacement d'agents spécifiques, il est facile de savoir qui traite davantage de commandes de remplacement que d'autres.

Toutes ces observations peuvent indiquer un risque potentiel de fraude. La solution analytique adaptée peut les identifier et vous alerter pour que vous puissiez ouvrir une enquête avant que les pertes n'atteignent des sommets.

Conclusion

Le professionnel chargé de la protection des actifs du commerce a aujourd'hui besoin d'outils novateurs et puissants pour déceler et éliminer les risques de fraude interne. Ces outils doivent par-dessus tout booster l'efficacité (vous permettre d'identifier et de résoudre rapidement les problèmes avant que les pertes ne se multiplient) et être performants (offrir un taux élevé d'alertes vraies positives) pour optimiser les compétences du personnel et accélérer les enquêtes. Prenez une longueur d'avance en adoptant une solution analytique avancée, comme l'analyse prescriptive, pour découvrir les cas de fraude les plus subtils et protéger vos marges et vos profits.

Pour en savoir plus sur l'analyse prescriptive et sur la façon dont elle aide le service de protection des actifs à lutter contre la fraude et la non-conformité, rendez-vous sur www.zebra.com.

Zebra
Prescriptive Analytics™

Powered by Zebra Savanna™