L'AGEFI HEBDO
TOUS LES MÉTIERS DE LA FINANCE

PAYS : France
PAGE(S) :28
SURFACE :87 %
PERIODICITE : Hebdomadaire

RUBRIQUE : Dossier big data
DIFFUSION :(20000)
JOURNALISTE : Alexandra Oubrier

► **3 novembre 2016 - N°538**

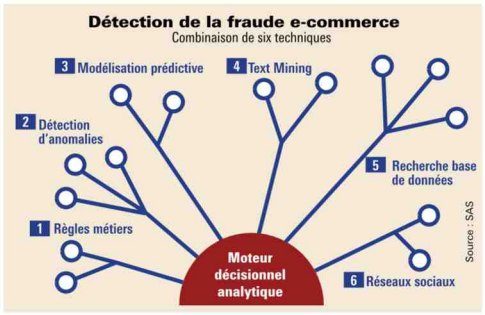
DOSSIER BIG DATA

Les données rendent la lutte contre la fraude plus efficace

L'utilisation de données externes et l'usage du « machine learning » donnent des perspectives nouvelles à la sécurisation des transactions.

PAR ALEXANDRA OUBRIER

En 2015, la fraude aux paiements a coûté 522 millions d'euros en France. Certes, le taux de fraude n'est que de 0,082 %, mais les deux tiers ont lieu lors de paiements à distance (*card not present*). « *Plus on dématérialise, plus la fraude augmente* », souligne Thierry le Forban, *product manager* chez Monext. Le recours à l'authentification renforcée s'est généralisé mais elle pèse encore sur le taux de conversion que surveillent de près les commerçants, c'est pourquoi les prestataires de services de paiement, y compris les banques, se dotent d'outils de détection de fraude de plus en plus innovants. La diffusion du *big data* et des technologies de *machine learning* contribue à améliorer l'efficacité de la lutte anti-fraude. Plus les données analysées sont volumineuses, plus les modèles de détection sont pertinents, et l'utilisation d'algorithmes auto-apprenants facilite leur mise à jour.



Evaluer le risque

C'est ce qu'a montré SAS, éditeur de solutions de *data management*, lors de son récent Forum annuel. « *L'important, c'est d'évaluer le risque et de suivre la fraude et son montant en temps réel pour pouvoir agir en priorité sur la fraude la plus coûteuse*, a expliqué Florence Giuliano, *fraud strategy director*. *La plate-forme SAS fournit un socle technique homogène et un large périmètre fonctionnel, elle agrège des données internes et externes à l'entreprise pour alimenter un 'datamart' dédié à la lutte anti-fraude.* » Là, SAS applique une approche hybride combinant jusqu'à six modules de détection de fraude : les règles métier spécifiques au domaine traité mais qui provoquent de nombreux faux positifs (alerte sur des transactions non frauduleuses), la détection d'anomalies qui doit être fréquemment mise à jour, la modélisation prédictive permet de repérer les modèles de fraude à partir d'un historique qui doit être de taille suffisante pour que la détection soit pertinente, le *text mining* encore peu utilisé dans l'e-commerce mais qui permet d'ajuster les scores de fraude produits par les modèles prédictifs, le croisement avec des bases de données (listes noires), l'établissement de réseaux sociaux (liens entre des personnes agissant en réseau) par le biais d'une adresse IP, d'un numéro de compte… En Belgique, BNP Paribas Fortis a lancé un projet pilote qui s'avère très performant : un milliard de transactions sont analysées chaque jour, ce qui génère moins de 200 alertes mais permet de détecter plus de 90 % de la fraude.

A côté de ces solutions industrielles, certaines de ces technologies sont utilisées par des intervenants plus petits mais tout aussi pointus. Younited Credit (ex-Prêt d'Union) par exemple a recruté Xavier Burtschell en tant que *chief data officer* pour affiner les techniques de détection de fraude. « *L'activité ayant démarré en 2011, nous disposons d'un historique suffisant pour faire parler les données*, explique-t-il. *Nous avons donc développé deux modèles prédictifs dont l'un à base de 'machine learning' qui intègre les données de comportement sur le web (provenance des internautes, saisie des demandes de crédit…) et devrait permettre d'affiner le score de fraude.* » La définition des modèles et leur ajustement sont la clé d'une détection efficace, mais nécessite du temps pour vérifier que les alertes générées correspondent bien à des cas réels de fraude. D'ailleurs, ces modèles sont utilisés en complément d'autres moyens de détection classiques.

Autre exemple, Payplug, présent auprès de 20.000 petits e-commerçants, a développé son propre outil de lutte contre la fraude à base de *machine learning*. « *Cela représente deux ans de travail et 2 millions d'euros d'investissement*, souligne Antoine Grimaud, cofondateur de PayPlug. *Notre logiciel traite des milliers de données en temps réel et peut déclencher 3D Secure en quelques millisecondes. Il apprend automatiquement, ce qui a permis de réduire le nombre de faux positifs et d'améliorer la satisfaction de nos clients.* » Outre les données classiques liées à la transaction, ce logiciel établit une « *empreinte digitale* » de l'appareil utilisé par l'internaute et peut l'ajuster si les données changent (nouvelle version du navigateur, par exemple). Cette empreinte est combinée à une analyse comportementale fondée sur la frappe du clavier, les fenêtres ouvertes ou fermées, les mots utilisés… ce qui améliore la précision du modèle. Un prototype actuellement en test auprès d'acteurs du paiement et de la banque donne de bons résultats.

La Poste a récemment racheté ProbaYes, une start-up de *data scientists* qui élabore des modèles et les teste auprès de ses clients, La Banque Postale et le Groupement Cartes Bancaires, pour la détection de fraude. Outre les historiques des clients, l'équipe cherche à intégrer des données exogènes (la météo, par exemple) pour tester leur pertinence. Le *machine learning* est très prometteur pour lutter contre la fraude mais nécessite encore du temps pour affiner les modèles. ■