



FRAUDFORUM²⁰¹⁹

2 JUILLET | Hôtel Le Bristol Paris, FRANCE



Comment Experian met en œuvre du Machine Learning pour répondre aux défis de la fraude

Frédéric Bomy
Senior data modeller manager, Experian

Les challenges

Une détection de la fraude à optimiser :

- Le coût de la fraude représente 5% du PIB monde
- Les techniques de fraude évoluent constamment :
« L'amélioration des techniques de fraude est beaucoup moins coûteuse, en temps et en argent, que celle des moyens de prévention. » (Bruno Lussato)
- La détection de la fraude ne doit pas aller contre l'expérience client (trop de faux positifs)



Pourquoi la data science peut aider à la détection de fraude



Des données **asymétriques** avec **très peu** de fraude



La **data science** permet de mettre en exergue plus efficacement des **comportements similaires de clients** (patterns de comportement normal et détection de comportement anormal) plutôt que de se baser uniquement sur l'historique du client ou d'identifier les scénarii de fraude.



Il permet de **réduire le nombre de faux positifs** et ainsi de **diminuer le nombre d'études manuelles et de refus**.



Il **complète** le système de règles en l'optimisant et en détectant plus efficacement la fraude et **améliore les process** d'automatisation.

L'approche data science de la fraude

Data

Les sources de données dépendent du **type de fraude et de la disponibilité des données** : données transactionnelles, données voix, données textuelles, ...

Méthode

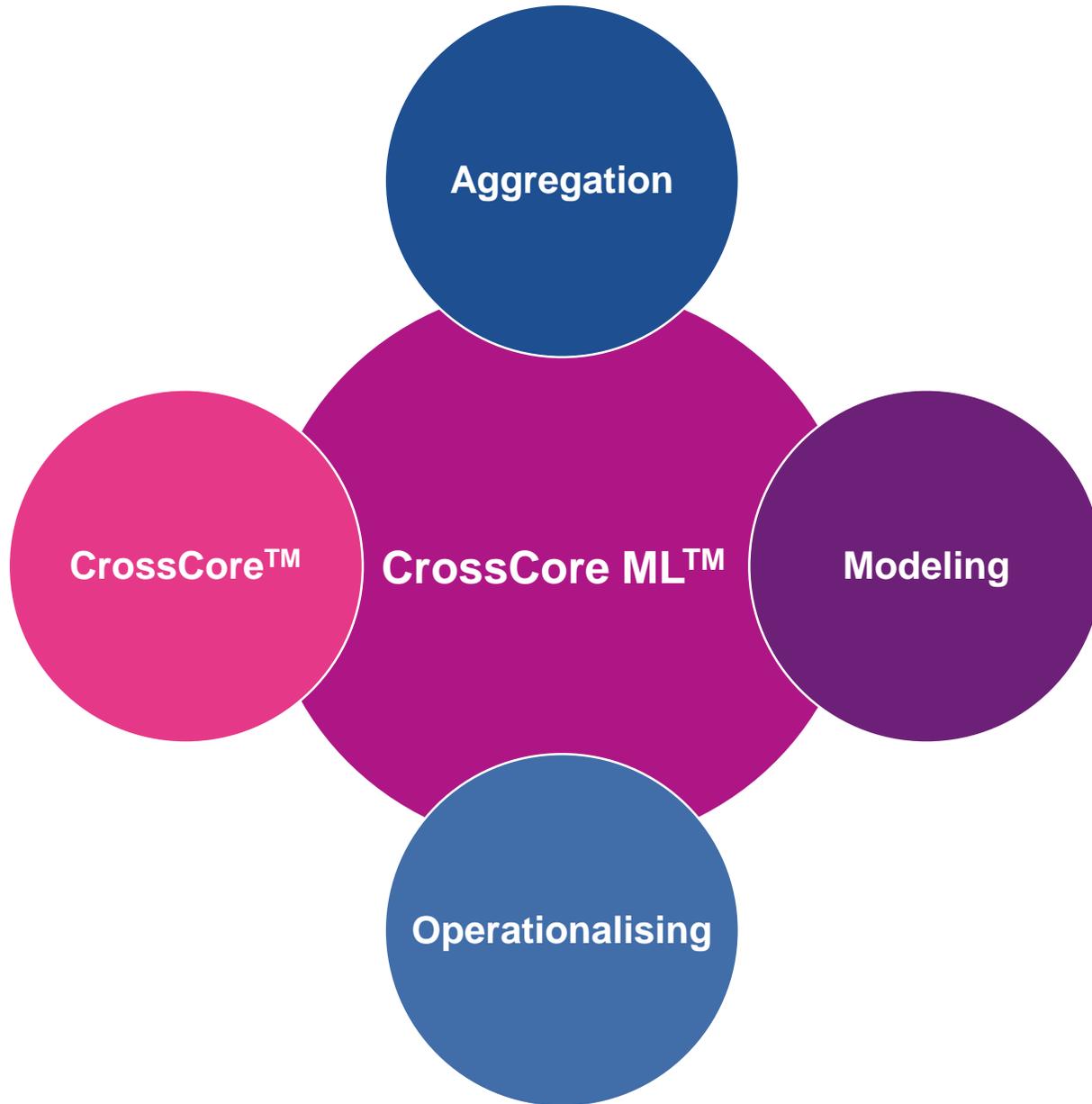
- Affiner les périmètre de modélisation : modèles imbriqués.
- Aller vers de nouvelles techniques de modélisation : SMOTE + ENN+ modèle d'ensemble, analyse textuelle, pattern analysis, anomaly detection, link-mining ...



- ✓ Une plus grande **flexibilité**
- ✓ Des méthodes spécifiques et appropriées pour détecter **différents types de fraude**
- ✓ Des méthodes qui détectent plus rapidement de **nouvelles familles** de fraude

Suivi et fine-tuning

- Les modèles d'analytique avancée doivent être adaptés aux pratiques des fraudeurs : suivi des règles et modèles
- L'optimisation régulière du modèle et des règles permet de diminuer le nombre de faux positifs.



Experian intègre le machine learning au sein de sa gamme via une composante spécifique : CrossCore Machine Learning

- Une plateforme de “data feed” en temps réel connectée à CrossCore
- Suite à l’application des règles, les données sont envoyées dans un environnement analytique
- Les modèles développés par les data scientists y sont disponibles



- Un environnement de développement complet à destination des data scientists y compris pour l’analyse exploratoire et le « tuning » des modèles
- Un environnement évolutif : installation simple de nouveaux outils (Tensorflow par exemple)
- Un déploiement simple des modèles développés



- Audit et évaluations des décisions
- Management du pipeline de décision du machine learning jusqu’à la prise en compte dans CrossCore

Pourquoi CrossCore™ machine learning?

Le service de Machine Learning de CrossCore:

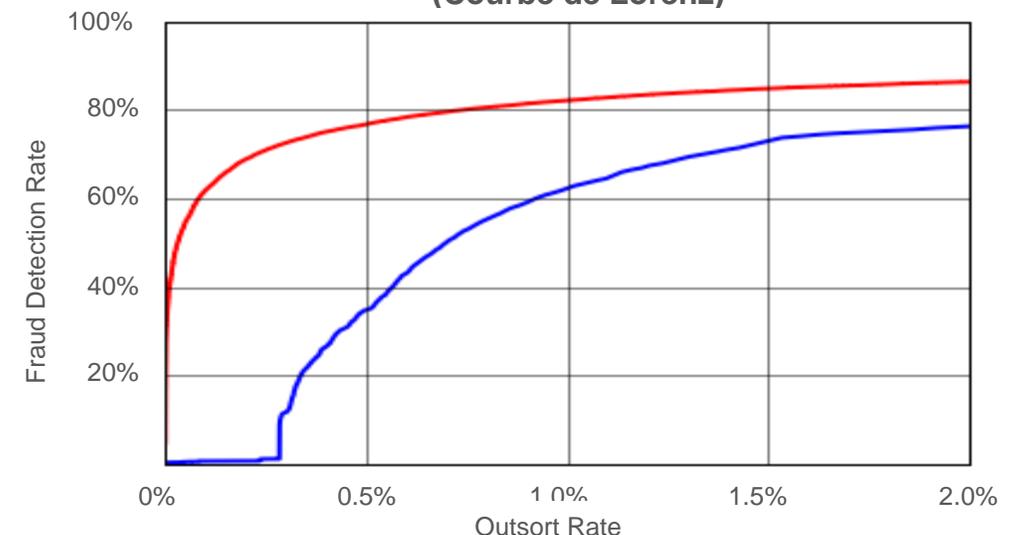
1. Permet de passer de prises de décisions disparates en matière de fraude et d'identité en une seule recommandation globale.
2. Exécute les modèles de manière transparente dans le cadre d'un workflow d'identité et de fraude.
3. Optimise la détection des fraudes en intégrant les données de tous les services d'Experian et de ses partenaires dans les modèles
4. Réduit les « faux positifs », diminuant les taux de révision manuelle sans diminuer la détection.
5. Contrôle les coûts et augmente l'efficacité en limitant le nombre de services nécessaires pour prendre des décisions en toute confiance.
6. Réduit la dépendance à l'égard du réglage manuel et des longs processus d'approbation de la gouvernance des modèles, permettant aux analystes de se concentrer sur les nouvelles attaques de fraude.

Cette étude de performance montre les résultats du modèle d'un client de vente au détail (courbe rouge) vs. résultats traditionnels basés sur des règles (courbe bleue).

En utilisant CrossCore ML, notre client conserve le même taux de détection de la fraude tout en **diminuant la revue manuelle de 74%**.

Cela se traduit par des approbations automatiques de **\$270 million**.

Comparaison ML aux résultats initiaux (jeu de règles)
(Courbe de Lorenz)



Le Machine Learning bénéficie de la puissance de CrossCore

Nous proposons des modèles génériques en fonction du contexte opérationnel.

Le Machine Learning se positionne comme la dernière brique de CrossCore et permet de capitaliser sur toutes les applications Experian et tierces.

**CrossCore for
Account Opening**

Demande de crédit / ouverture de compte ... sur tous canaux
Fraude : usurpation d'identité, d'identifiant ...
Solutions utilisées : Hunter, Fraudnet, Emailage

**CrossCore for
Account Registration**

Accès à un compte existant... sur canal digital
Fraude : usurpation d'identifiant
Solutions utilisées : Fraudnet, Biocatch

**CrossCore for
Risk-Based Authentication**

Transaction à partir d'un compte existant sur canal digital
Fraude : usurpation d'identifiant, usurpation d'identité
Solutions utilisées : Fraudnet, Biocatch, Boku

**CrossCore for Online &
Mobile Fraud Detection**

Accès à un compte existant/ création de compte sur canal digital
Fraude : usurpation d'identité, d'identifiant ...
Solutions utilisées : Fraudnet, Biocatch, Boku, Emailage

**CrossCore for Identity
Verification and Proofing**

Accès à un compte existant/ ouverture de compte sur tout canal
Fraude : usurpation d'identité, d'identifiant ...
Solutions utilisées : Fraudnet, Mitek, Boku, Emailage

**CrossCore for Application Fraud
Detection and Data Consortium**

Ouverture de compte sur tout canal
Fraude : usurpation d'identité, d'identifiant ...
Solutions utilisées : Hunter, Fraudnet, Emailage

La solution de fraude multicouche intégrée de CrossCore

Etude de cas d'une plateforme multinationale de commerce électronique

Les challenges de Radial

Le plus grand fournisseur de commerce omnicanal au monde doit gérer le risque de fraude tout en développant son activité sur des marchés notoirement à risque. Cela a conduit à:

- Une augmentation des attaques de fraudeurs, des chargebacks et des faux positifs,
- Augmentation significative des coûts opérationnels pour soutenir l'expansion
- Un risque de fidélité à la marque en hausse puisque leurs meilleurs clients sont frustrés par des refus

... en conséquence, Radial s'est presque immédiatement retiré de ces opportunités d'expansion du marché.

Notre approche: Plate-forme technologique CrossCore, outils de fraude en couches et analyses avancées

Nous avons rapidement intégré une combinaison plus efficace d'outils de fraude et pris une décision de risque consolidée: intelligence d'identité, évaluation du risque de courrier électronique et gestion du risque de fraude pour le commerce électronique, ainsi que des modèles d'apprentissage automatique permettant de prendre des décisions de risque intégrées en temps réel dans CrossCore. Nous avons également été en mesure de fournir de meilleurs renseignements aux fins de l'examen par les enquêteurs.

Les conséquences pour Radial

- Les revenus ont augmenté grâce aux approbations automatiques à faible risque
- Les rejets de débit pour fraude ont diminué de manière significative
- Les coûts opérationnels pour maîtriser le risque de fraude sont restés stables
- Radial a renforcé la confiance de la marque en générant plus de commandes avec moins chargebacks



CrossCore a contribué à la stratégie de Radial visant à réduire les chargebacks et à améliorer l'efficacité opérationnelle :

Diminution des chargebacks
~ **40%**

Estimation des économies annuelles résultant de la réduction des chargebacks
~ **\$5,000,000**

ROI estimé: **7 : 1**

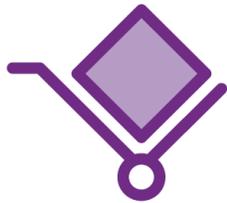
CrossCore™ Machine Learning



Rapidité



Adaptabilité



Facilité



Précision



Les services Partenaires connectés sur CrossCore

DONNEES ALTERNATIVES

Augmente la couverture des contrôles et la performance des vérifications d'identité / appréciations des risques de fraude.



BIOMETRIE



- Solutions de biométrie faciale, fingerprint, voix, ...
- Solutions de biométrie passive ou comportementale

Entrée en relation, usurpation de compte



CONTROLE DOCUMENTAIRE

Vérification de l'intégrité des documents d'identité.
Validation par selfie avec détection "liveness".



SURVEILLANCE DE RESEAUX

Surveillance temps réel de réseaux téléphonique pour les fraudes centre d'appels.



CHARGEBACKS MANAGEMENT

Gestion intégrée des chargebacks pour le e-commerce.

