

Factsheet – Fusion Global PAYplus

Détection et prévention de la fraude pour Fusion Global PAYplus

L'Intelligence Artificielle (IA) au service de la détection et de la prévention de la fraude en temps réel



La problématique de la fraude

La fraude est devenue une menace croissante pour les banques et leurs clients, coûtant des milliards de dollars chaque année. Les fraudeurs utilisent désormais l'ingénierie sociale pour commettre diverses escroqueries telles que les fraudes à la fausse facture, la fraude au président ou compromettre les messageries d'entreprises.

Certaines banques ont décidé de rembourser leurs clients, mais d'autres mettent en cause directement la responsabilité de leurs clients pour avoir initié la transaction. Dans les deux cas les profits de la banque et la confiance du client en l'institution sont impactés.

Quels sont les dés rencontrés par les banques avec les solutions basées sur les moteurs de règles?

- Les règles détectent uniquement les scénarios de fraudes identifiés par le passé, ne protégeant pas la banque contre les nouveaux scénarios de fraude.
- Les moteurs de règles génèrent un nombre élevé de faux positifs qui nécessitent de nombreuses ressources pour investiguer chaque transaction suspecte.
- Le besoin de mise à jour et de configuration continue des règles engendre des coûts importants en ressources humaines.

- Les plaintes de clients pour la non-détection de leurs transactions frauduleuses ou du blocage trop fréquent de leurs transactions légitimes sont très courantes.

Comment surpasser les règles avec l'IA

L'intelligence artificielle permet aux banques de détecter plus précisément les fraudes tout en minimisant les faux positifs. NetGuardians est une fintech suisse spécialisée dans la prévention de la fraude bancaire. Sa solution de lutte contre la fraude reconnue et basée sur l'IA fonctionne en modélisant le comportement normal de paiement de chaque client et utilise des modèles de risques comportementaux pour détecter les transactions frauduleuses, en dehors du comportement usuel du client. Les cas de fraudes sont détectés au niveau des comptes clients grâce à la combinaison de facteurs transactionnels tel que le montant, le bénéficiaire, le pays destinataire, la devise, le type d'ordre etc.

Les paiements bloqués peuvent être investigués au travers d'un tableau de bord compréhensible pour chaque type d'utilisateur. L'approche innovante de NetGuardians permet aux banques de se prémunir contre les paiements frauduleux en temps réel mais également de détecter avec précision les nouveaux scénarios de fraude.

Comparé aux solutions basées sur un moteur de règles, les banques souscrivant à la solution NetGuardians pourront :

- Réduire le nombre de fausses alertes de 83%
- Augmenter la détection de la fraude de 18%
- Réduire de 93% le temps nécessaire à l'investigation
- Accéder au partage avec la base de données de l'Intelligence Artificielle NetGuardians pour une meilleure évaluation du type de fraude auxquelles elles sont confrontées

L'acquisition et l'implémentation d'une solution basée sur l'IA requière habituellement l'intervention de nombreuses ressources pendant plusieurs mois. Grâce à FusionFabric.Cloud votre banque peut en être équipé en seulement une semaine

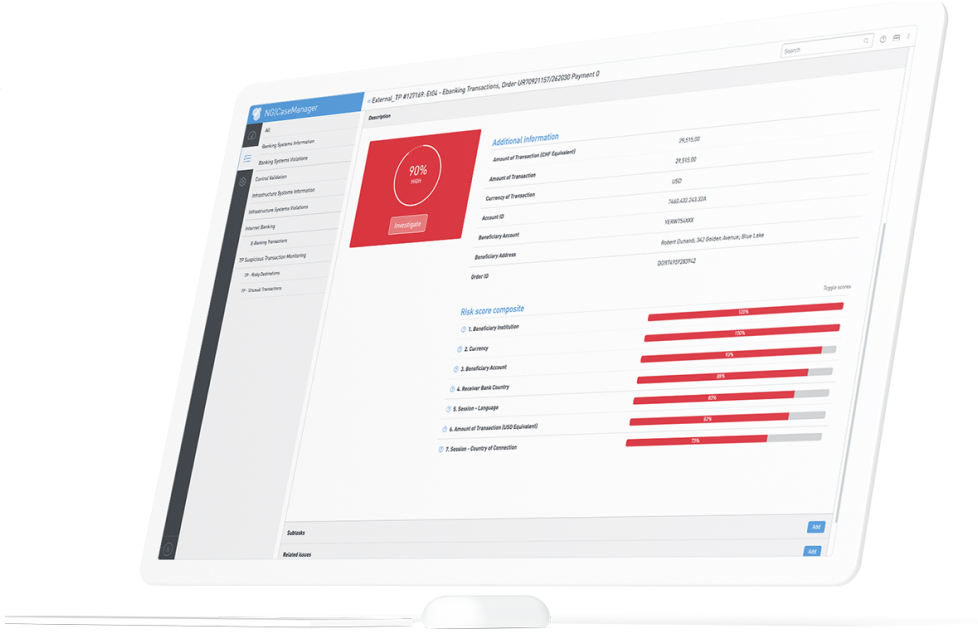
Avantages liés à FusionFabric.Cloud :

- L'application est hébergée et gérée par Finastra, libérant vos ressources informatiques.
- Processus de diligence effectué par Finastra et des évaluateurs tiers.
- Le support est le même que celui de Fusion GPP, permettant une vue globale sur les installations et facilitant les interventions en cas de dépannage.
- Les banques peuvent tirer parti de l'« IA Collective » et améliorer la précision de l'évaluation du risque et ainsi réduire davantage le nombre de faux positifs.
- Le filtre anti-fraude intervient en moins d'une seconde grâce à l'hébergement réalisé sur l'environnement de GPP.
- La solution fonctionnera avec toutes les mise à jour GPP futures, évitant toute interruption.

- La solution peut être activée en une semaine pour réduire rapidement les coûts de gestion inhérents à la gestion du risque de fraude et augmenter la satisfaction de vos clients.

Etapas à suivre pour l'activation

- Approuver l'offre financière (coût unique d'installation et coûts récurrents basés sur le volume de transactions annuelles).
- Signature du contrat d'abonnement Finastra.
- Autoriser le partage des données de paiement avec la communauté Finastra Fusion afin de prévenir et détecter les transactions frauduleuses (optionnel).
- Configuration de la solution y compris les modèles de risque IA sur la base de l'historique des paiements.
- Activation et mise en service.



About Finastra

Finastra is building an open platform that accelerates collaboration and innovation in financial services, creating better experiences for people, businesses and communities. Supported by the broadest and deepest portfolio of financial services software, Finastra delivers this vitally important technology to financial institutions of all sizes across the globe, including 90 of the world's top100 banks. Our open architecture approach brings together a number of partners and innovators. Together we are leading the way in which applications are written, deployed and consumed in financial services to evolve with the changing needs of customers. Learn more at finastra.com

Finastra and the Finastra 'ribbon' mark are trademarks of the Finastra group companies.
© 2020 Finastra. All rights reserved.

Corporate Headquarters

4 Kingdom Street
Paddington
London W2 6BD
United Kingdom
T: +44 20 3320 5000

