mind FINTECH

PAYS : France
PAGE(S) :7-8
SURFACE :160 %
PERIODICITE : Hebdomadaire

JOURNALISTE : Christophe Auffray

► **21 janvier 2021 - N°184**

Floa s'attaque à la fraude téléphonique grâce à l'analyse vocale

Floa Bank, ~~ex-Banque Casino,~~ est déjà équipé de technologies de lutte contre la fraude sur le Web. Depuis quelques mois, elle détecte également les tentatives de fraude sur le canal téléphonique. Pour cela, la banque s'appuie sur l'analyse du contexte d'appel. Retour sur ce projet mené avec l'éditeur Pindrop.

Filiale de Casino et du Crédit Mutuel, Floa Bank (~~ex-Banque Casino~~) compte en 2020 plus de 3 millions de clients. Elle en vise 5 millions à l'horizon 2025 grâce à son expansion en Europe. Cette croissance l'expose cependant parallèlement à un risque accru de tentatives de fraudes.

Jusqu'à présent, et en raison de son développement en ligne auprès d'e-commerçants, le web était le principal canal en termes de lutte contre la fraude. Mais les clients peuvent également contacter leur prestataire par le biais du téléphone. Et ce canal n'échappe pas non plus à ces pratiques, comme l'entreprise a pu le constater.

De 1 sur 300 à 1 sur 2 000 appels de fraudeurs

À combien se monte le préjudice annuel pour Floa ? Ces données resteront confidentielles. La perte est tout cas suffisante pour justifier des investissements technologiques permettant de mieux lutter contre ces attaques par téléphone.

"L'industrie est attaquée dans un ratio qui va d'un appel sur 300 à un appel sur 2000, en fonction du secteur, banque, assurance ou e-commerce. 90% des sociétés se situent dans cette fourchette. Si vous avez un million d'appel par an, vous pouvez déterminer combien émanent de fraudeurs. Calculez combien vous perdez en moyenne par appel frauduleux et vous obtenez une estimation de son coût annuel", résume Jean-Baptiste Boix, responsable fraude et cybercriminalité de l'entreprise.

La lutte contre la fraude doit respecter un complexe équilibre et ne pas affecter trop fortement l'expérience client - soit l'activité commerciale.

Or pour tromper les banques, les escrocs ne manquent pas d'astuces. Ils profitent également des procédures en place dans ces entreprises. La lutte contre la fraude doit respecter un complexe équilibre et ne pas affecter trop fortement l'expérience client – soit l'activité commerciale. *"Nous étions vraiment face à une véritable problématique. Nous devions satisfaire* ■■■

Les éléments clés du projet

Date de début du projet : les premières discussions ont été engagées en fin d'année 2019, la procédure de déploiement du projet a été mise en action au début de l'année 2020.

Durée de l'expérimentation et du déploiement : en tant que pionnier de cette solution en France, Floa Bank a dû étudier le contexte législatif et harmoniser la solution avec la règlementation en vigueur ce qui a demandé un temps d'action complémentaire. En temps normal, on peut se baser sur une mise en place inférieure à un semestre.

Date de mise en production : la solution a été mise en production courant novembre 2020.

Nombre de personnes impliquées dans le projet : le projet a nécessité l'implication d'équipes transverses au sein de Floa et d'un groupe de travail côté Pindrop, soit une dizaine de personnes.

mind FINTECH

PAYS : France
PAGE(S) :7-8
SURFACE :160 %
PERIODICITE : Hebdomadaire

JOURNALISTE : Christophe Auffray

► **21 janvier 2021 - N°184**

■■■ *deux enjeux : minimiser les pertes financières et maximiser l'expérience client. Et seule la technologie permettait de le faire*", souligne l'expert de la banque.

Limiter les pertes sans ajouter de frictions pour le client

Pas question donc de confronter le client lors d'un appel à d'interminables questions afin de confirmer son identité. Cela ne serait pas non plus la garantie d'une protection à 100 %. Les pirates disposent de stratagèmes éprouvés pour collecter des données authentiques auprès des victimes.

"Nous nous sommes plutôt orientés vers des signaux de défiance. Plutôt que de reconnaître le client, on cherche à identifier l'appel qui ne ressemble pas à l'appel légitime du client", explique Jean-Baptiste Boix (Floa)

Un exemple : la mise en ligne sur un site d'annonces gratuites populaire en France d'une fausse offre pour un appartement au loyer très attractif. Arguant de l'examen des dossiers des loueurs, les fraudeurs obtiennent ainsi copies de pièces d'identité, RIB et bulletins de paie. Ces informations leur serviront dans un second temps, entre autres, à ouvrir des lignes de crédit auprès de banques.

La communication de données exactes n'atteste donc pas pour les conseillers de Floa Bank d'être au téléphone avec de vrais clients. Pour réduire son exposition à la fraude téléphonique, l'établissement a donc déployé en 2020 une solution dédiée de détection de l'éditeur Pindrop.

Celui-ci a pour le moment choisi de faire l'impasse sur une technologie de reconnaissance biométrique, trop contraignante sur le plan de la conformité au RGPD. *"Nous nous sommes plutôt orientés vers des signaux de défiance. Plutôt que de reconnaître le client, on cherche à identifier l'appel qui ne ressemble pas à l'appel légitime du client"*, explique Jean-Baptiste Boix.

1 500 critères pour établir un score de fraude

La solution Pindrop apporte ainsi une identification unique du terminal ou du contexte d'appel. L'éditeur vérifie par exemple le modèle de smartphone utilisé, mais aussi plusieurs de ses composants techniques. Il s'agira par exemple de la version d'iOS pour un iPhone.

L'opérateur téléphonique sera lui aussi pris en compte dans la détection. À chaque opérateur correspond en effet un bruit de fond spécifique. Grâce à l'analyse de ce paramètre, la banque peut contrôler que le client appelle toujours depuis son fournisseur habituel. Ces critères ne suffisent pas néanmoins.

En tenant compte du contexte d'appel, comme le lieu où il est passé (y compris la pièce de la maison), il est possible de renforcer encore la protection contre la fraude. En tout, ce sont près de 1 500 critères différents qui seront analysés afin d'établir un score de confiance, communiqué aux téléconseillers. *"Ils donneront une coloration fraude ou non à l'appel au travers d'incohérences d'appel"*, précise Jean-Baptiste Boix.

Pour concevoir ces modèles de détection de la fraude, Pindrop et son client s'appuient donc sur l'examen des appels dits à froid. Ce terme désigne l'historique des appels enregistrés. L'exploitation de ces données explique d'ailleurs l'importance du volet réglementaire d'un tel projet de lutte contre la fraude.

Un volet RGPD majeur à prévoir dès le début du projet

"C'est un point d'attention dès le début pour maximiser l'efficacité et minimiser la durée d'exécution du projet. Le RGPD est une partie importante à anticiper", insiste le responsable fraude et cybercriminalité. Si un pilote était opérationnel en trois à quatre mois, la conformité est venue "retarder" la mise en production.

Cela explique aussi que Floa Bank ait préféré différer l'adoption de la reconnaissance biométrique et se concentrer sur le spectre acoustique de l'appel plutôt que la voix. Le service fraude est ainsi en attente d'une validation du département conformité pour avancer sur la biométrie vocale. Se posera alors un autre enjeu.

La finalité de la détection de fraude, rappelle Jean-Baptiste Boix, est aussi de ne pas ajouter de frictions client. *"Une fois que ce type de technologie est en place et maîtrisé, il s'agit aussi de proposer au client un meilleur accueil et de pouvoir lui rendre service plus rapidement."*

En comparaison, l'enrôlement par la biométrie reste complexe, pour des raisons réglementaires, mais aussi d'expérience client. Une signature vocale de l'ensemble des clients doit être captée et conservée avec son consentement, par le biais d'une plateforme d'enrôlement. ■

Christophe Auffray