L'ANGE GARDIEN DES PORTEURS DE CARTE

Savoir doser sa présence visible au service du client.

Zoom sur l'équipe Lutte contre la fraude (LCLF) de BPCE Payment Services

L'équipe LCLF de BPCE Payment Services paramètre des systèmes de détection automatique de la fraude, analyse les alertes, et contacte les porteurs de carte pour effectuer des levées de doute et minimiser les préjudices si nécessaire. Elle remplit cette mission pour des établissements bancaires au sein du Groupe BPCE comme en-dehors, de même que pour des commerçants en ligne. En parallèle, elle coopère aussi avec les autorités publiques et de place.

Le mythe de l'ange gardien traverse l'histoire religieuse, littéraire et folklorique. Ce personnage, bien qu'invisible, reste toujours vigilant à l'arrière-plan. Il écarte les dangers de ceux qu'il a pris sous son aile. Une métaphore, bien-sûr, mais qui illustre l'un des paradoxes de l'expérience client : le meilleur service au client doit savoir parfois s'effacer, pour n'apparaître qu'aux moments opportuns.

C'est un principe simple à énoncer, mais qui exige, pour être mis en œuvre, à la fois une profonde empathie et d'importants moyens techniques. L'équipe LCLF joue ce rôle d'ange gardien pour tous les porteurs de cartes Banque Populaire, Caisse d'Epargne mais aussi les porteurs de cartes de dizaines d'autres banques qui sous-traitent leur monétique en marque blanche au Groupe BPCE.

L'équipe LCLF est ainsi responsable de déjouer les tentatives de fraude sur plus de 2 milliards d'opérations par carte bancaire chaque année. Découvrez dans cet article l'approche et les méthodes des anges gardiens !

UNE ÉQUIPE DE **45** PERSONNES

DONT

25 ANALYSTES RISQUES

ET

DES DATA SCIENTISTS

1 OPPOSITION DE CARTE TOUTES LES **2MIN.**

100 ÉTABLISSEMENTS BANCAIRES PROTÉGÉS

DONT

15 POUR LE COMPTE DESQUELS L'ÉQUIPE LCLF GÈRE LE PROCESSUS DE BOUT EN BOUT

Y COMPRIS LES APPELS AUX PORTEURS DE CARTES

UNE VEILLE **24h/7/365**

17 MILLIONS DE CARTES BANCAIRES EN CIRCULATION

2.3 MILLARDS DE DEMANDES D'AUTORISATION TRAITÉES PAR AN

1 MILLION D'ALERTES AUTOMATIQUES ANALYSÉES PAR AN

160 MILLIONS D'EUROS DE FRAUDE ÉVITÉE PAR AN

Un subtil équilibre pour minimiser la gêne du client

La majorité des opérations par carte bancaire, paiements ou retraits, font d'abord l'objet d'une demande d'autorisation. On s'en rend rarement compte, sauf à regarder de près ce qu'affiche le terminal de paiement lorsqu'on paie dans un magasin. C'est à ce stade qu'intervient l'équipe LCLF, en temps réel.

La validation d'une opération s'opère en fait en deux temps. D'abord, sont vérifiées les règles de base : que la carte bancaire du porteur ne soit pas expirée, qu'elle n'ait pas été mise en opposition, que le compte bancaire du porteur soit suffisamment crédité, etc. Ensuite, avec ces conditions remplies, un algorithme d'analyse des risques vérifie si la transaction correspond à un schéma de fraude connu.

Par exemple, si des opérations de retrait ont lieu dans un laps de temps très court, dans plusieurs pays étrangers, les données de la carte bancaire ont sans doute été clonées – c'est ce que les spécialistes appellent « l'ubiquité ». Lorsque l'algorithme détecte une fraude présumée, il bloque automatiquement l'opération et déclenche une alerte. Cette alerte est alors examinée par un analyste risque. Ce dernier s'appuie sur le contexte – lieu de la transaction, moment de la journée, montant, habitudes du porteur de cartes – pour décider, soit de la considérer comme une fausse alerte, soit de réaliser une levée de doute en appelant le porteur de carte. S'il n'arrive pas à le joindre, il peut bloquer à titre préventif certains types de paiement afin de limiter la gêne occasionnée tout en protégeant le porteur.

« Nous devons systématiquement mettre en balance les différentes sources de gêne potentielles pour les clients, explique Carine Meriot, manager de l'équipe LCLF en charge de la fraude porteur. La plus grande gêne serait bien-sûr d'être victime d'une fraude. En revanche, si un client se retrouve en vacances avec une carte bloquée à mauvais escient, il sera très incommodé aussi. Nous nous efforçons d'être un ange discret, mais bien présent. »

Pour cette raison, confier le traitement des alertes à un analyste « en chair et en os » reste incontournable. Tatiana Jochemczak, Gestionnaire Middle Office BPCE Payment Services. détaille : « Seul un expert fraude peut déterminer que, non, ce n'est pas incohérent d'avoir un paiement dans une station essence à Paris, puis un achat dans un magasin de matériel musical à Londres quelques minutes plus tard. Ce dernier peut correspondre à une vente en ligne. Une hypothèse qu'on peut valider en constatant que le client a déjà acheté chez ce commerçant quelques mois plus tôt. »

Par ailleurs, un autre aspect permet de réduire les inconvénients pour le porteur de carte : l'intégration des différents maillons du paiement. Le fait d'être, comme le Groupe BPCE, à la fois émetteur de cartes bancaires, gestionnaire des terminaux et solutions de paiement chez les commerçants, ainsi que processeur des opérations de paiement, permet une authentification plus rapide et plus fiable. « Lorsque l'authentification prend trop longtemps, ou pire, qu'elle échoue, c'est une source de frustration aux caisses des magasins physiques. Pour les commerçants en ligne, c'est aussi le risque de laisser échapper une vente – leur concurrent n'est qu'à un clic, rappelle Carine Mériot. Des solutions de paiement intégrées minimisent ces désagréments pour les clients et ces aléas pour les marchands. Cela nous permet de proposer des environnements à la fois fluides et sécurisés aux porteurs de cartes et à nos partenaires commerçants, par exemple dans le cadre de l'authentification forte prévue par la réglementation DSP2. »

L'interaction client en situation de tension : souplesse et compréhension

L'interaction avec les clients reste irremplaçable pour réaliser une levée de doute ou décider d'une mise en opposition de carte. « Nous intervenons dans des situations génératrices de stress pour le porteur de carte, décrit Tatiana Jochemczak, Gestionnaire Middle Office BPCE Payment Services. Nous devons les écouter, les rassurer, et faire preuve d'agilité pour les aider à résoudre leurs problèmes. Je me souviens par exemple d'un homme d'affaire qui, au début de la crise du Covid, avait sa carte bloquée dans un aéroport à l'étranger, en raison d'une fausse alerte, alors qu'il voulait acheter un billet d'avion pour rentrer au plus vite. L'échange était initialement très tendu, mais lorsqu'il a compris que nous mettrions tout en œuvre pour qu'il soit sur le prochain avion, Il nous a remercié longuement ».

Cette qualité de service ne doit rien au hasard : les analystes risques sont recrutés, outre leurs compétences techniques, pour leur sensibilité relationnelle. Les échanges téléphoniques avec les porteurs de cartes sont enregistrés et les incidents, heureusement rares, font l'objet d'une investigation systématique pour ajuster les scripts téléphoniques et offrir, le cas échéant, du coaching et de la formation aux analystes. Une large palette d'indicateurs de qualité fait l'objet d'un suivi constant.

En coulisses, une course perpétuelle contre les fraudeurs

Mais une part essentielle de la vigilance des équipes de Lutte contre la Fraude restera totalement invisible du grand public. Il s'agit de la détection des nouvelles formes de fraude, ainsi que des échanges continus avec l'écosystème bancaire et judiciaire.

En effet, les fraudeurs ne cessent « d'innover ». Dans les équipes Lutte Contre la Fraude, une équipe répertorie et ajuste chaque jour les règles face aux nouveaux modes opératoires des fraudeurs. Elle scrute en permanence les flux de transaction à la recherche de nouveaux schémas de fraude. Une mission très technique, à laquelle contribue l'équipe de data scientists de BPCE Payment Services. Ce sont des spécialistes de la modélisation des risques et de l'intelligence artificielle. Les data scientists simulent également les effets qu'entraînerait la mise en place de nouvelles règles de détection automatique des fraudes présumées. Néanmoins, les outils technologiques ne suffisent pas : la dimension psychologique et l'expérience sont essentiels. Comme l'explique Tatiana Jochemczak, Gestionnaire Middle Office BPCE Payment Services : « Nous savons par exemple que les fraudeurs cherchent à exploiter les craintes et angoisses de leurs cibles. Dès le début de la pandémie de Covid-19, nous nous attendions à voir apparaître des schémas de fraude autour de la fourniture de gel hydroalcoolique ou de masques. Les fraudeurs surfent aussi astucieusement sur l'actualité. Dans les tentatives d'escroquerie par « phishing[1] » , les fraudeurs adaptent aussi leurs messages à la période de l'année : ils cherchent par exemple à se faire passer pour les services fiscaux en période de déclaration d'impôt. »

Théo LOPES-QUINTAS - *data scientist*

> ***Les data scientists conçoivent et produisent des algorithmes de machine learning pour compléter le travail de détection et de protection des analystes métier. Ces outils d'aide à la décision permettent aux analystes de confirmer ou d'infirmer leurs intuitions.***

[1] Le « phishing », ou hameçonnage, est une technique de fraude dans laquelle un escroc se fait passer pour un tiers de confiance et incite la victime à lui communiquer des informations confidentielles, par exemple, un numéro et/ou un code de carte bancaire.

Le point de vue de Thomas Roth, Directeur de la Lutte Contre la Fraude et du Risk Management, et de Florence Covemaeker, Responsable Fraud Management, de BPCE Payment Services.

Quelles tendances notables observe-t-on dans le domaine de la lutte contre la fraude ?

On assiste depuis plusieurs années à une sophistication croissante des attaques, à laquelle répond une hausse de la compétence et de l'expertise des équipes chargées de les déjouer. Les attaques sont protéiformes et combinent des vecteurs technologiques et humains. Les fraudeurs profitent aussi de la multiplication des situations de paiement, en ligne et dans le monde physique, pour exploiter les moindres failles. Face à eux, nous renforçons constamment l'arsenal, avec de notre côté aussi, une surenchère technique et de nouveaux outils comme le machine learning.

> ***Nous sommes le dernier rempart. Ce qui nous conduit à refuser environ 0,3 % des opérations sur un total de 2,3 milliards de transactions monitorées chaque année.***

Observe-t-on aussi des évolutions de la part des clients ?

Oui, aussi bien chez les commerçants que chez les porteurs de carte, on constate plusieurs phénomènes : d'abord, un fort besoin de sécurité et de réassurance – on touche presque à l'intime avec la sécurité des paiements. Ensuite, une multiplication des exigences, avec des parcours et des situations de paiement de plus en plus variés : le multicanal, les cartes de paiement virtuelles, les cartes préenregistrées, le sans contact, etc. Dans toutes ces configurations, commerçants et porteurs aspirent à la fluidité maximale, sans transiger bien entendu sur le niveau de sécurité. Enfin, on observe chez certaines catégories de clients la volonté d'être actifs et autonomes dans la gestion de leur propre sécurité. C'est pour répondre à ces attentes que nous développons des plateformes digitalisées, où les clients peuvent paramétrer eux-mêmes leurs critères de sécurité, dans des limites définies par leur banque.

Comment se transforment vos équipes pour répondre à ces impératifs et demandes ?

Elles montent en compétence et intensifient les coopérations transverses. Nos équipes comprennent de plus en plus de spécialistes des données, d'architectes IT, de spécialistes du digital, qui recoupent leurs points de vue pour offrir aux porteurs de carte une expérience simple et sécurisée.

Face à des adversaires aussi sophistiqués, la coopération est de mise. Elle fait partie intégrante des missions de l'équipe LCLF, que ce soit avec d'autres institutions financières (sociétés émettrices de cartes bancaires et banques) ou avec les autorités judiciaires. Dès qu'un nouveau schéma de fraude est identifié, l'information est partagée le plus vite possible pour limiter les préjudices. Et par la suite débute une procédure de longue haleine pour aider à appréhender les fraudeurs et recouvrer une partie des sommes détournées.

Assurer une protection efficace et discrète à l'arrière-plan, se manifester pour aider et rassurer au bon moment : les deux facettes de la mission ne sont pas contradictoires, mais complémentaires pour une expérience client optimale.

Pour avoir ce coup d'avance, les anges LCLF bénéficient d'une masse de données sans équivalent en France qui couvre l'ensemble du territoire, de technologies de pointe pour faire tourner des algorithmes de machine learning en quelques millisecondes et d'échanges permanents d'information en interne et en externe. C'est cela et une énergie de chaque jour qui permet de protéger sans importuner.

NOTRE EXPERT

Carine Meriot
Lutte Contre La Fraude & Risk Management

Se protéger contre la fraude

La vigilance de l'équipe LCLF n'exclut pas la prudence. Fidèles à leur mission de prévention, les experts vous rappellent quelques bons réflexes, que vous ayez une carte protégée par eux ou non :

1 Ne pas sous-estimer les fraudeurs. La fraude ne touche pas que des victimes crédules ou mal informées. Et les messages des fraudeurs ne sont pas toujours ineptes ou écrits en mauvais français.

2 Ne communiquez jamais vos données confidentielles. Votre banque connaît déjà les informations liées à votre carte bancaire et ne vous les demandera jamais.

3 Refusez de confirmer une opération sur votre application bancaire si ce n'est pas vous qui l'avez initiée. Des escrocs prétextent parfois que votre confirmation est nécessaire pour bloquer une opération frauduleuse ou obtenir un remboursement. C'est un leurre.

4 Vérifiez l'identité des sites de e-commerce. Privilégiez les sites sécurisés, reconnaissables au préfixe https dans leur adresse URL. Avant d'acheter en ligne, contrôlez systématiquement que l'adresse du site correspond : les fraudeurs montent parfois de faux sites de toute pièce.

5 Paramétrez les opérations autorisées. La plupart des banques proposent aujourd'hui de fixer soi-même des critères d'autorisation, via son application bancaire. On peut par exemple exclure d'office certains pays ou certaines catégories de sites internet. Ces critères peuvent être changés quasi instantanément : on peut donc très bien débloquer un pays étranger avant de s'y rendre en vacances, puis le bloquer à nouveau à son retour.

6 Au moindre doute, n'hésitez pas à vous rapprocher de votre chargé de clientèle bancaire. Ils sont à votre écoute.