COMARCH

LIVRE BLANC

La fraude aux programmes de fidélité

Sommaire

Introduction

Abonnements, fidélité émotionnelle et sociale, données zero party, gamification, hyperpersonnalisation... voici quelques-unes des tendances et buzzs qui apparaissent aujourd'hui dans les articles, la presse ou lors de conférences lorsqu'on parle de fidélité. Les programmes de fidélité ne cessent d'évoluer et un nombre toujours plus important d'entreprises décident de lancer leurs propres programmes.

Cette tendance trouve son origine dans la difficulté grandissante à suivre, collecter et analyser les données clients. Avec l'élimination progressive des cookies tiers et l'introduction de législations strictes sur la confidentialité des données dans un nombre croissant de pays dans le monde, les programmes de fidélité restent un des rares leviers permettant de recueillir des données clients de qualité.

Cependant, un aspect de la gestion des programmes de fidélité reste inchangé : les programmes de fidélité sont des mannes à exploiter pour les fraudeurs, les cybercriminels et les joueurs. De fait, les nouveaux acteurs qui explorent les opportunités liées au lancement de leurs propres programmes de fidélité, tout en éliminant progressivement l'utilisation des cookies tiers, s'exposent également à des risques de fraudes élevés.

Malgré un début de prise de prise de conscience des enjeux, les grands défis demeurent inchangés : l'impact de la fraude est encore sous-estimé par la majorité des directions et il n'existe pas de méthode bien définie pour mesurer le retour sur investissement des outils de prévention de la fraude. Ainsi, le challenge de trouver l'équilibre entre expérience client aboutie, mécaniques de fidélité simples et éprouvées et sécurité, n'a jamais été aussi prégnant.

La fraude aux programmes de fidélité : une définition floue

Alors que les programmes de fidélité deviennent de plus en plus courants, les organisations sont confrontées à un certain nombre de défis différents.

À quels défis les entreprises se retrouvent-elles confrontées aujourd'hui dans la lutte contre la fraude à la fidélité ?

L'un des principaux problèmes de la fraude à la fidélité est l'absence de définition formelle, contrairement à la fraude par carte de crédit ou encore de paiement. Ces fraudes par carte de crédit / paiement font l'objet de réglementations légales et utilisent des méthodes de détection et de prévention bien établies, qui sont toutes largement comprises et partagées.

Les organisations ont du mal à fournir une explication universelle de ce que signifie la fraude à la fidélité, car elle peut varier en fonction de la structure d'un programme de fidélité et de la manière dont les clients sont récompensés.

Au lieu d'essayer de trouver une définition générique qui couvrirait toutes les activités frauduleuses possibles, il faut distinguer les types les plus courants de fraude à la fidélité en déterminant les parties impliquées et les motivations de leur action frauduleuse.

Les trois types de fraude à la fidélité les plus courants

Fraude interne

Fraude commise par des acteurs internes, tels que le personnel du site, les administrateurs du programme, les agents du centre de contact, les partenaires et les intégrateurs, qui exploitent leurs privilèges d'"initiés" contre les systèmes informatiques ou les conditions du programme.

Fraude externe

Fraude sous forme de prise de contrôle de comptes, d'usurpation d'identité, d'ingénierie sociale et d'attaques par botnet.

Fraude "gaming"

Également appelée "fraude amicale", il s'agit d'une fraude commise par un membre ou un utilisateur qui exploite une faille à des fins personnelles, notamment des boucles d'accumulation, des rachats non autorisés, des défauts d'intégration ou une mauvaise configuration des processus.

Quantifier les pertes engendrées par la fraude à la fidélité

Un problème partagé par les programmes de fidélité de tous les secteurs d'activité est celui de la quantification des pertes dues à la fraude. Sans une mesure universelle des pertes, il est difficile de justifier les dépenses liées aux outils de prévention de la fraude et de persuader la direction d'investir dans la sécurité des programmes de fidélité. Comment les entreprises pourraient-elles créer une équipe dédiée à la prévention de la fraude s'il n'est pas possible d'analyser le rapport coût-bénéfice ?

Il n'existe pas de réponse simple à cette question, mais répondre aux questions suivantes pourrait aider :

- Quel est le coût par point dans le programme ?
- Existe-t-il un mécanisme standard de facturation des points/récompenses ?
- Quel est le coût estimé d'acquisition des membres ?
- Les coûts du programme sont-ils centralisés ou répartis entre les sites ou partenaires ?
- Quelle est la valeur moyenne de la CLV (Customer Lifetime Value) pour les membres du programme de fidélité ?

Parallèlement à l'analyse des réponses à ces questions, il est important de prendre en compte les chiffres clés suivants*

33%
des membres souhaiteraient rester dans le programme mais s'attendent à ce que les points ou les miles soient remplacés

17%
des membres disent qu'ils cesseraient toute activité avec une marque après une violation des données d'un programme de fidélisation

81%
des membres associent les points de fidélité à des bénéfices financiers

72%
des responsables de programmes de fidélisation ont rencontré des problèmes liés à la fraude

93%
des personnes interrogées disent préférer les programmes de récompense qui ont des mécanismes de prévention de la fraude

26%
disent qu'ils annuleraient leur adhésion au programme de récompenses après un incident de fraude à la fidélité

* Source: Connexions Loyalty Report, N=1600 shoppers

Expérience client Versus sécurité

Un autre défi pour les équipes en charge de la fidélisation est de trouver un équilibre entre la sécurité de leur programme et l'expérience client. Il est évidemment possible de mettre en œuvre des mesures telles qu'une authentification à deux facteurs obligatoire pour chaque connexion, la génération d'un mot de passe unique chaque fois qu'un membre souhaite effectuer un échange ou encore la mise en place d'une politique de mot de passe complexe. En fait, de nombreuses équipes de sécurité aimeraient avoir toutes ces mesures mises en place, car elles permettraient de réduire efficacement les activités frauduleuses. Cependant, la mise en œuvre de toutes ces mesures serait trop lourde à supporter pour certains membres fidélisés. Il faut donc trouver un compromis entre d'un coté l'expérience client et de l'autre la sécurité.

Malheureusement, trouver le juste milieu entre les deux peut se révéler difficile. La bonne nouvelle est qu'il existe des outils et des méthodes facilement accessibles qui peuvent faire la différence.

Une de ces méthodes est l'A/B testing, qui consiste à sélectionner un petit groupe témoin (de membres ou d'utilisateurs) et à vérifier comment ce dernier réagit à une nouvelle méthode de sécurité avant de la déployer à tous les membres / utilisateurs. Les géants de l'internet comme Facebook, Twitter et Google effectuent constamment des milliers d'A/B test sur leurs applications. Ce n'est qu'après s'être assurés que la modification proposée n'a pas d'impact négatif sur l'expérience et la fidélisation des utilisateurs qu'ils la diffusent à grande échelle.

Piratage des comptes

Même si l'abus des règles ou le « gaming » du système de fidélité peut ne pas être considéré comme une fraude grave par certains, le vol ou l'achat d'identifiants de comptes divulgués sur le Dark Web est généralement considéré comme contraire à l'éthique et illégal.

Malheureusement, les programmes de fidélité sont souvent la cible de ces attaques. En général, les programmes de fidélité sont dotés de mesures de sécurité plus faibles que les systèmes bancaires, par exemple. De plus, les usagers réutilisent leurs mots de passe sur plusieurs comptes et il suffit d'une seule fuite de données d'identification pour déclencher une vague de prises de contrôle de comptes dans plusieurs entreprises. Mais la vérité est que ce ne sont pas les points ou les récompenses que ces acteurs recherchent : il s'agit avant tout de données personnelles qu'ils peuvent soit corréler avec d'autres informations volées à d'autres sources, soit simplement utiliser pour d'autres abus.

La prise de contrôle de comptes et l'usurpation d'identité peuvent être très rentables, d'autant plus qu'ils peuvent souvent être entièrement automatisés et/ou cryptés.

COMPTES	
Cartes-cadeaux de retailer en ligne	15-50% DE LA VALEUR
Comptes bancaires en ligne	0,5%-10% DE LA VALEUR
Compte de service Cloud	5–10$
Comptes de messagerie piratés (2 500)	1–15$
Compte d'achats retail	0.50–99$
SERVICES DE TRANSFERT D'ARGENT ET CARTES DE CRÉDIT	
Service de redirection des liquidités pour les comptes bancaires	1-15% DE LA VALEUR
Service de redirection de l'argent liquide pour un système de paiement en ligne	1-5% DE LA VALEUR
Payez 100$ en bitcoins et recevez un transfert d'argent de 1000$.	100$
Service de redirection des fonds	5-20% DE LA VALEUR
Carte de crédit unique	0.50–20$
Une seule carte de crédit avec tous les détails (fullz)	1–45$
IDENTITÉS	
Identité volée ou fausse	0.10–1.50$
Notes médicales et ordonnances	15–20$
Compte en ligne pour téléphone portable	15–25$
Scans ou modèles de pièces d'identité/passeports	1–35$
Packs d'identification complets	30–100$
Fausse carte d'identité, permis de conduire, passeport, etc.	25–5,000$
LOGICIELS MALVEILLANTS ET SERVICES	
Générateur de téléchargement de macros Office	0.10–1.50$
Boîte à outils des *„Cheval de Troie"* bancaires courants avec prise en charge	15–20$
Spyware	15–25$
Service de blanchiment d'argent (en espèces ou en crypto-monnaies)	1–35$
Service de retrait	30–100$
Pirate informatique professionnel	25–5,000$
Service de page de phishing personnalisé	25–5,000$
Service DDoS, courte durée <1 heure	25–5,000$

* Source: Symantec ISTR24

Au nombre des nouvelles tendances pour contrer les prises de contrôle de comptes, figure l'authentification sans mot de passe et l'authentification continue.

Les smartphones actuels ont popularisé l'utilisation de l'authentification biométrique, par le biais de techniques de reconnaissance des empreintes digitales et du visage. Une technique qui est communément considérée comme supérieure aux mots de passe traditionnels. Plus encore, s'ils sont utilisés correctement, les front-ends peuvent être une source de quantités massives de données sur l'utilisateur final. Il peut s'agir de données de base telles que les adresses IP, la localisation et le type de données du navigateur web, mais aussi des données plus avancées telles que les schémas de frappe et l'activité de navigation sur les sites web.

L'utilisation de ces données combinée au machine learning permet de détecter les activités suspectes en temps réel et, par exemple, de ne demander une authentification à deux facteurs que si le comportement de l'utilisateur est très différent de l'historique enregistré. De cette façon, les comptes susceptibles d'avoir été usurpés peuvent être rapidement bloqués pour vérification, tandis que les comptes sans aucune activité suspecte ne sont pas soumis à de contrôles de sécurité supplémentaires.

Fraude interne

Les équipes de sécurité chargées de créer et de maintenir les outils et les procédures pour protéger les programmes de fidélité ont tendance à se concentrer uniquement sur les menaces externes, alors que souvent, le plus grand risque se trouve au sein même de l'organisation : in fine, ce sont les employés qui font fonctionner le programme de fidélisation. Il y a toujours un risque que ces derniers - les administrateurs, les analystes, les agents du service clientèle et le personnel sur site (boutique, magasin) - soient eux-mêmes les fraudeurs, ce qui comporte un risque beaucoup plus élevé que les menaces extérieures. Si de nombreuses organisations sont conscientes des risques posés par les agents externes, la plupart négligent les agents internes.

La fraude interne est une préoccupation croissante, surtout si l'on considère que le service client lié à la fidélisation est couramment externalisé. Si l'on ajoute à cela un taux de rotation du personnel relativement élevé, il est clair que les centres de contact et les opérations d'assistance à la clientèle doivent faire l'objet d'une surveillance constante, avec des procédures de signalement appropriées et des voies d'escalade clairement définies.

Également, la mise en en place de process de contrôles basiques peut être un moyen simple mais efficace de réduire le risque de fraude interne. Par exemple, le superviseur du centre de contact doit approuver certaines opérations à risque (telles que les corrections manuelles de points ou les transferts importants de points) etc.

Une autre méthode efficace pour réduire le risque de fraude interne consiste à mettre en place un ensemble de procédures opérationnelles standards pour la fraude liée à la fidélité. Ces procédures sont généralement très courantes pour les fraudes liées aux paiements ou aux rétro-facturations, mais malheureusement, très peu d'organisations en disposent et les maintiennent pour leurs opérations fidélité.

Les procédures opérationnelles standards doivent répondre aux questions suivantes :

- Qui ou quelle équipe est officiellement responsable de la prévention et de la détection des fraudes en matière de fidélité ?
- Quels sont les indicateurs clés de performance et les statistiques à suivre régulièrement pour détecter rapidement les anomalies dans le programme de fidélité ?
- Quelle procédure une fois l'activité frauduleuse découverte ?

La surveillance des données et les audits inopinés ont permis de fortes réductions des pertes et une diminution de la durée de la fraude.

Pertes réduites de
52%

Surveillance et analyse des données

Détection
58%
plus rapide

Pertes réduites de
51%

Audits surprises

Détection
54%
plus rapide

Les fraudeurs avec le plus d'ancienneté dans l'entreprise volent deux fois plus

Plus de 5 ans d'ancienneté : 200 000 $ de perte médiane

Moins de 5 ans d'ancienneté : 100 000 $ de perte médiane

Au cours des 10 dernières années, le nombre de poursuites pour fraude professionnelle a diminué de 16%.

La crainte d'une mauvaise publicité est la principale raison de l'absence de poursuite

* Source: ACFA 2018 GLOBAL STUDY ON OCCUPATIONAL FRAUD AND ABUSE

Fraude à l'inscription

L'un des principaux domaines touché par la fraude à la fidélité est l'acquisition de nouveaux membres. L'acquisition de nouveaux membres est souvent l'un des principaux indicateurs clés de performance pour les équipes marketing ou en charge du CRM / de la fidélisation. C'est pourquoi elles créent des incitations pour faire adhérer les nouveaux membres, comme par exemple :

- **Récompenses immédiates,** telles qu'un coupon unique ou un bon de réduction pour les nouveaux membres.
- **Les bonus d'inscription,** qui récompensent les membres pendant une période déterminée après leur inscription - par exemple, un programme peut doubler le nombre de points attribués pour l'activité d'un membre pendant le premier mois de sa participation.
- **Les mécaniques de parrainage,** qui récompensent les membres qui parrainent de nouveaux entrants dans le programme.

Les fraudeurs comprennent ces mécanismes et ciblent les systèmes de fidélisation avec diverses méthodes pour créer de nouveaux comptes frauduleux dans le but de mettre la main sur les avantages associés. La façon la plus logique de défendre les programmes de fidélisation contre les inscriptions frauduleuses serait de mettre en place un arsenal d'outils et de processus autour du nouveau processus d'inscription, comme par exemple :

- Mise en œuvre de CAPTCHAs, de mots de passe à usage unique ou d'une authentification à deux facteurs.
- Mise en place d'une politique de mot de passe stricte, par exemple en créant une règle selon laquelle les membres doivent changer leurs mots de passe tous les 6 mois.
- Collecte de données personnelles supplémentaires au cours du processus d'inscription, par exemple l'adresse du domicile ou un numéro de document officiel (tel que le numéro de sécurité sociale ou le numéro de passeport) afin de valider les données personnelles par rapport aux bases de données officielles.
- Mise sur liste noire des adresses IP ou des domaines de messagerie suspects.

Certaines de ces techniques sont essentielles pour la sécurité de base du système. Cependant, chacun de ces outils ajoute un certain niveau de complexité au processus d'inscription des membres, ce qui augmente le taux de rebond et a un effet négatif global sur l'expérience des nouveaux membres.

Analyse de cas 1

Un opérateur de programmes de fidélité à grande échelle du Royaume-Uni a introduit une récompense instantanée pour les nouveaux membres, à savoir un bon de réduction de 10%. Peu après la mise en place de cette mesure incitative, le nombre de nouveaux membres est passé à environ 1 000 jusqu'à 7 000 nouveaux comptes par jour, contre quelques centaines auparavant.

Quelques semaines plus tard, l'équipe marketing a reçu une alerte de l'équipe sécurité, indiquant que les bons de réduction, ainsi que les informations d'identification des comptes de fidélité, avaient fait l'objet de transaction sur le dark web.

Ils ont entamé une enquête interne en examinant les nouvelles inscriptions et ont découvert qu'environ 15 % d'entre elles avaient été créées à l'aide de données personnelles fausses ou générées artificiellement, ou encore via des boîtes mail jetables (plus connues sous le nom de « Messagerie électronique temporaire » ou « Disposable email address »)

Exemples de données de comptes frauduleux

Prénom	NOM DE FAMILLE	ADRESSE EMAIL
Addhjhy	JHUSUU	CILOB43916@ABBUZZ.COM
Sdkuyuio	QEIOUY	IYMYQWME@SHARKMAIL.COM
Breuyeuu	WIUYPI	IYMYQWME@POKEMAIL.NET

L'opérateur de fidélité a introduit des listes noires supplémentaires de domaines de messagerie, mais les fraudeurs ont simplement utilisé de nouvelles listes. Finalement, il a été décidé d'invalider une série de nouveaux bons de réduction avec la conséquence suivante : près de 45 % des nouveaux membres légitimes n'ont plus jamais interagi avec le programme.

Analyse de cas 2

Après avoir mis à jour les règles de son programme de fidélité et introduit un ensemble plus varié de récompenses, un acteur du secteur pétrolier et gazier d'Amérique Latine a commencé à recevoir un nombre croissant de plaintes de ses membres qui ne pouvaient pas se connecter à leur compte.

Ils ont par la suite découvert une violation des données dans les systèmes de l'un de leurs partenaires et l'exposition d'un grand nombre d'identifiants de connexion. Malheureusement, certains de leurs membres utilisaient le même mot de passe sur le site web du partenaire et sur leur compte de fidélité.

Les données ont fuité de la base de données du partenaire de l'opérateur de fidélisation : et après ?

- Des robots d'indexation recherchent massivement et automatiquement d'autres sites où les mêmes séries d'informations d'identification donnent accès à d'autres systèmes.

- Dès le moment où ils obtiennent un accès, ils utilisent l'adresse électronique légitime pour en créer une nouvelle en ajoutant un préfixe ou un suffixe différent à l'adresse email originale.

Exemples :

EMAIL FUITE DU MEMBRE	CHANGEMENT D'ADRESSE E-MAIL
John.brown@gmail.com	JOHN.BROWN_EBY1@GMAIL.COM
honeybun@yahoo.co.uk	HONEYBUN_EBY1@YAHOO.CO.UK
bruhh@outlook.com	BRUHH_EBY1@OUTLOOK.COM

- Après ça, ils changent le compte de fidélité volé associé à l'adresse électronique par le nouveau compte..
- Enfin, ils proposent des identifiants de compte comportant des points de fidélité à vendre sur le dark web.

Tout le processus décrit ci-dessus se déroulait de manière entièrement automatisée via des bots et des scripts. Bien que la violation des données n'ait pas eu lieu à partir du système de l'opérateur de fidélisation, l'entreprise a constaté une augmentation du taux de désabonnement des clients et une dégradation importante de son image.

Solution : Le service de sécurité des inscriptions

Chez Comarch, nous avons sécurisé le process des inscriptions grâce à l'intelligence artificielle (IA). Notre Service de Sécurité des Inscriptions propulsé part l'IA est entraîné sur des données historiques pour détecter les nouvelles inscriptions ou les modifications de données personnelles frauduleuses. Il analyse chaque nouvelle inscription ou modification de données personnelles à l'aide d'un ensemble de modèles statistiques et de modèles de traitement du langage naturel par apprentissage automatique.

Il détecte en temps réel :

- Si les données personnelles utilisées pour l'inscription ont été générées artificiellement ;
- Si une adresse électronique inhabituelle ou jetable est utilisée ;
- S'il y a un pic dans les inscriptions de nouveaux membres, ce qui peut indiquer qu'une campagne massive d'inscriptions frauduleuses est en cours ;
- Si les données personnelles utilisées lors de l'enregistrement sont répétées à plusieurs reprises.

De cette façon, nous pouvons empêcher la création de nouveaux comptes frauduleux, mais aussi les prises de contrôle de comptes existants.

Aucune règle n'est à paramétrer, une configuration minimale suffit : le service examine toutes les inscriptions entrantes ou les changements de données personnelles et les classe comme suit :

1. Inscription légitime

2. Fraude potentielle

- Avec une explication de la raison pour laquelle le compte a été signalé comme potentiellement frauduleux, et une demande d'examen manuel
- Ces comptes peuvent, par exemple, être autorisés à accumuler des points, mais ceux-ci ne peuvent pas être utilisés avant que leur statut ne soit confirmé

3. Frauduleux

- Avec une explication de la raison pour laquelle le compte a été signalé comme frauduleux

Le Service de Sécurité des Inscriptions via l'IA peut être déployé et intégré de manière transparente à d'autres solutions Comarch ou tierces via messages ou API Web. L'ensemble de la solution peut être livré pour des tests d'intégration en quelques jours à partir du partage des données historiques pour la formation de modèles de machine learning.

Comment sécuriser votre programme ?

Nous avons traité la thématique de la fraude à la fidélité sous bien des aspects, mais une question essentielle demeure : comment protéger votre programme de la fraude ?

5 étapes pour maximiser la protection de votre programme de fidélité contre la fraude

1. Établir des responsabilités claires pour la gestion et la prévention de la fraude à la fidélité

Il peut s'agir d'un individu ou d'une équipe, mais désigner un chargé des « risques liés à la fraude à la fidélité et de la prévention » est essentiel. Dans le cas contraire, la responsabilité de ce périmètre devient floue et il n'est pas possible d'éviter les renvois de responsabilités entre les différents services : équipe commerciale responsable du programme, IT, juridique ou conformité, en charge de l'évaluation des risques, ou encore service clientèle.

Nous recommandons de conserver la gestion et la responsabilité de la fraude à la fidélité au sein de l'équipe responsable du programme de fidélité (généralement une équipe du département marketing). Les activités opérationnelles peuvent être transférées au service clientèle, voire à une autre équipe déjà chargée de la fraude et/ou de la conformité sur d'autres sujets dans l'entreprise (généralement paiements et rétro facturations).
Toutefois, ce n'est qu'en gardant la responsabilité de la fraude à la fidélité au sein de l'équipe qui gère le fonctionnement et les performances du programme au quotidien, qu'il sera possible de s'assurer que la fraude et sa prévention seront prise en compte de manière appropriée lors des discussions autour de la stratégie du programme et de son exécution.

2. Créer un ensemble de règles et de limitations simples dans le cadre de la logique commerciale du programme.

Une fois que les responsabilités sont clairement définies, il est temps de créer un ensemble de limites et de seuils simples qui serviront de fondation à la stratégie de prévention de la fraude. Voici quelques exemples :

- Limiter le nombre de rédemptions (de points) pouvant être effectués par un client en un jour, une semaine ou un mois.
- Créer une alerte si le nombre d'inscriptions de nouveaux membres dépasse de 30 % la moyenne quotidienne ou hebdomadaire du programme.
- Définir une règle empêchant les agents du service clientèle de procéder à des ajustements manuels excessifs des points.
- Autoriser uniquement les rédemptions (de points) pour les membres qui ont fourni toutes les données personnelles requises par le programme et confirmé 2 canaux de communication (par exemple, l'adresse e-mail et le numéro de téléphone).
- Signaler et vérifier manuellement les comptes des membres qui modifient leur mot de passe ou leurs données personnelles après une longue période d'inactivité.

Dans votre choix de fournisseur de logiciel de fidélité, assurez-vous que des limites et des règles comme celles mentionnées ci-dessus peuvent être facilement créées, modifiées et mises à jour sans frais supplémentaires.

3. Créer des indicateurs clés de performance mesurant l'exposition à la fraude, qui sont contrôlés et vérifiés régulièrement

Les bases étant posées, l'étape suivante consiste à créer un ensemble de contrôles réguliers pour s'assurer que rien d'inhabituel ne se produit dans le programme. Voici un ensemble type de métriques à vérifier régulièrement :

- La base des membres – répartition des comptes des membres selon leur statut d'activité, niveaux statutaires, acquisition de nouveaux membres sur les différents canaux.
- Le ratio des ventes faites aux membres fidélisés vs. non fidélisés.
- Les points accumulés et échangés sur les différents canaux, partenaires et sites.
- L'activité des membres – nombre de vérifications du solde de points, de réinitialisations du mot de passe, de modifications des données personnelles, de corrections et d'ajustements manuels de points, d'annulations de transactions.

Il est important de recouper ces métriques avec les tendances et les promotions du moment. Dans tous les cas, la détection d'une anomalie dans l'une de ces métriques à l'échelle du programme doit sonner l'alarme et déclencher une enquête. De plus, il est nécessaire d'avoir au moins une estimation approximative de la valeur monétaire de votre opération de fidélisation. Quel est le coût du point échangé avec le partenaire ? Quel est le coût moyen d'acquisition d'un membre ? Chaque transaction de fidélisation doit être évaluée – c'est le seul moyen de suivre correctement le coût de la fraude dans le programme. C'est aussi la meilleure façon de s'assurer de l'intérêt des décideurs pour le programme de prévention de la fraude et de garantir ainsi des budgets.

4. Etablir une procédure standard de gestion de la fraude

Avoir défini des responsabilité claires, des KPIs et des limites est un bon début, cependant, que devrait-il se passer lorsqu'une réelle activité frauduleuse est découverte ? Quelles devraient-être les priorités de communication et les voies d'escalade ? Quelle équipe devrait-être impliquée ? Quelles mesures disciplinaires devraient être envisagées si une action frauduleuse provient de l'intérieur de l'organisation ? Ce ne sont là que quelques-unes des questions auxquelles il convient de répondre dans les procédures opérationnelles standard de fraude à la fidélité. La meilleure façon de l'aborder est de reprendre l'ensemble des procédures existantes et de les adapter aux exigences de fidélité. L'idéal est de partir d'un ensemble de processus de base décrivant ce qui devrait se passer une fois qu'une activité frauduleuse est découverte en se basant sur les scénarios les plus évidents. Et ensuite de s'assurer que ces procédures sont régulièrement mises à jour au fur et à mesure de la détection de nouvelles fraudes.

5. Envisager l'automatisation et la mise en place des bons outils

En considérant les quatre étapes ci-dessus, la conclusion qui vient à l'esprit est probablement : "c'est beaucoup de travail". Et c'est vrai. Surtout si l'on considère qu'aucune de ces étapes n'est ponctuelle : pour que l'ensemble du processus fonctionne, toutes ces étapes doivent être régulièrement révisées et répétées. Ces actions mettent à rude épreuve les équipes chargées de gérer les programmes de fidélité.

Par conséquent, le partenariat avec le bon fournisseur technologique et le choix du bon ensemble d'outils jouent un rôle crucial. La plupart des activités de détection et de prévention de la fraude peuvent être automatisées avec succès à l'aide de moteurs de règles standard, de mécanismes de rapport et d'alerte, mais aussi de systèmes d'IA/machine learning. Ils permettent non seulement de maintenir les mesures de prévention de la fraude configurées manuellement, mais aussi de mettre en évidence de manière proactive de nouvelles anomalies et des schémas de fraude nouveaux ou inédits.

Conclusion

Bien que la fraude à la fidélité suscite de nombreuses questions, une chose est sûre : elle ne va pas disparaître et ne disparaîtra probablement jamais. Les organisations qui gèrent des plateformes de fidélité à grande échelle doivent s'attaquer frontalement à la fraude à la fidélité si elles veulent protéger leurs clients les plus précieux et leurs résultats. Dans le même temps, elles doivent tenir compte de l'équilibre précaire entre la sécurité et la meilleure expérience client possible. Le simple fait d'investir dans des mécanismes de sécurité sans tenir compte de la satisfaction globale des membres fidélisés peut également avoir des conséquences néfastes.

Le sujet de la fraude à la fidélité est complexe et souvent négligé, notamment par les directions. Ce n'est qu'en leur fournissant des définitions appropriées, des cas documentés et des chiffres concrets prouvant que la fraude peut entraîner des pertes financières importantes, qu'il est possible d'attirer suffisamment l'attention et d'obtenir ainsi l'adhésion de la direction et de l'organisation toute entière.

COMARCH

A propos de Comarch

Comarch accompagne les entreprises de toutes tailles et de tous secteurs dans l'amélioration de leur efficacité commerciale, l'établissement de relations solides et pérennes avec leurs partenaires et clients ainsi que dans la réduction des coûts d'exploitation. Comarch s'appuie sur des solutions innovantes, à la fois intégrées et ouvertes, et compte parmi ses clients des entreprises référentes dans leur secteur telles que Auchan, Les Galeries Lafayette, BP, Carrefour, Leroy Merlin, Kiloutou ou encore PMU. Nous aidons les entreprises à créer de la valeur en fournissant des solutions IT porteuses de sens, en prise directe avec les attentes des consommateurs.

contact@comarch.fr | www.comarch.fr | 03.62.53.49.00