LEARNING NUGGET
#5

Compliquer les escroqueries par carte

Les transactions frauduleuses: introduction et informations pour les combattre avec succès

La carte de débit est et reste un moyen de paiement très sûr. Grâce aux technologies les plus récentes, les moyens de paiement actuels (p. ex. sur terminal de magasin) s'accompagnent d'un taux de fraude extrêmement bas. Vu toutefois l'emploi des cartes dans le e-commerce, le thème de la fraude sans carte physique gagne constamment de l'importance. La plupart des types de fraude en effet visent le plus faible maillon de la chaîne: le titulaire de la carte lui-même.

Introduction

L'usage abusif des cartes, appelé également ci-après «fraude» ou «escroquerie», est une escroquerie accomplie ou une tentative de fraude commise à l'aide d'une carte de paiement telle que p. ex. une carte de crédit ou de débit. L'objectif des escrocs peut être de se procurer des marchandises, des prestations ou de l'argent liquide. La fraude par carte de paiement est aussi vieille que les cartes elles-mêmes. Au début, ces fraudes se produisaient uniquement lors des transactions en présentiel avec la carte (également désignées par transactions en face à face).

Depuis qu'il est possible d'utiliser les cartes comme moyens de paiement pour régler des achats en ligne dans le cadre du e-commerce (commerce électronique) et comme de plus en plus de titulaires de carte utilisent cette fonction, la fraude par cartes de paiement s'est décalée vers les transactions en distanciel avec la carte et les transactions en ligne.

- **Carte en présentiel («card present») – environ 6% de toutes les transactions frauduleuses:** lorsque la carte physique est utilisée (transaction basée sur ruban magnétique ou puce) pour acheter quelque chose sur place, p. ex. à un bancomat, dans un magasin, un restaurant, un bar ou un supermarché.
- **Carte en distanciel («card not present» – CNP) – environ 94% de toutes les transactions frauduleuses:** lorsque seules sont utilisées les données de la carte sont utilisées, mais que la carte physique n'est pas présentée au vendeur par l'acheteur. Exemples : saisie manuelle des données sur un terminal dans un magasin, au téléphone ou sur Internet.

Grâce à des systèmes de prévention modernes apprenant en permanence et à des règlements très étudiés, grâce aussi aux longues années d'expérience des analystes des fraudes et experts spécialisés, ces types de fraude peuvent être fortement endigués.

Utilisation croissante du e-commerce avec répercussion sur les comportements frauduleux

En 2018, 10% du total des transactions dans le monde étaient réalisées en ligne; jusqu'en 2022, les dépenses effectuées dans le e-commerce représenteront 17% de tous les chiffres d'affaires mondiaux (source: Ravelin Insights).

En 2020, les transactions en ligne ont à nouveau été en nette augmentation, entre autres à la suite du confinement pendant la pandémie du coronavirus. Au cours de cette période, une forme modifiée de comportement frauduleux a été observée, confirmée par des analyses internes réalisées par les prestataires acquéreurs Worldline et SIX. Tandis que le nombre de transactions frauduleuses augmente dans l'ensemble, le montant moyen de la fraude par transaction a diminué comparé aux années précédentes. Les fraudeurs adaptent habilement leur mode opératoire aux habitudes de paiement des titulaires de carte, ce qui rend la fraude plus difficile à détecter. Citons à titre d'exemple la «combine» du «hungry fraudster». Il s'agit là de commandes faites auprès de prestataires de service de livraison alimentaire à domicile et portant chaque fois sur plusieurs petits montants qui sont toutefois étalés de manière ciblée sur plusieurs jours. L'intention est, selon les circonstances, que le débit des montants ne soit pas détecté ou qu'il ne le soit que tardivement.

En matière d'usage abusif des cartes, il est question d'une course permanente entre les fraudeurs d'une part, et les prestataires de services de paiements d'autre part. Les fraudeurs recherchent toujours de nouveaux moyens de frauder; les émetteurs et les acquéreurs sont, quant à eux, constamment mis au défi de prendre de nouvelles mesures de protection et de déjouer les tentatives de fraude.

Les fraudeurs et leurs «combines»

Le Darknet, terme à la mode s'il en est, désigne un réseau anonyme qui représente une face cachée du public Internet. Les escrocs – les fraudeurs comme nous les appelons – peuvent interagir entre eux sous couvert de l'anonymat et tentent ainsi d'échapper à la police. Sur le Darknet, les escrocs vendent et achètent des données de carte et échangent des informations sur la façon de commettre une fraude et au sujet des outils à utiliser. Il s'agit là d'une forme croissante de criminalité organisée qui a son propre modèle commercial et une division efficace du travail.

Quels facteurs favorisent cette forme de criminalité?

L'occasion et des barrières d'accès basses: télécharger dans l'anonymat un navigateur adéquat, accéder aux sites appropriés du Darknet et effectuer un achat de données de cartes en cryptomonnaie est relativement simple.

Évolution des structures: l'image du pirate malin qui arrive à prendre le contrôle d'un serveur grâce à des compétences hors norme est en partie dépassée. L'usage abusif de cartes est désormais une infraction pénale qui ne nécessite pas de connaissances ou de compétences particulières, mais simplement la saisie de données sur des sites Web ou dans des applis. On constate que l'ensemble du secteur se professionnalise de plus en plus et qu'il propose de véritables packs de prestations de services qui, outre des logiciels malveillants programmés, contiennent tout ce qu'il faut pour mener à bien une attaque contre des pirates informatiques.

Absence de stigmatisation: toute une génération a grandi avec le téléchargement gratuit de films, de musiques, de jeux et delogiciels. La frontière entre les activités légales et illégales n'est pas toujours évidente et l'on peut ainsi avoir moins de scrupules à commettre une fraude en ligne.

Un usage insouciant des données à caractère personnel, en particulier sur les réseaux sociaux: les fraudeurs à la carte bancaire adorent surfer sur les réseaux sociaux pour capter les données personnelles de titulaires de cartes. Des exemples de ce type de fraudes sont listés ci-dessous dans «Ingénierie sociale». D'où l'importance cruciale que les titulaires de cartes prennent des mesures de sécurité fondamentales et qu'ils usent de prudence dans la gestion et la révélation de leurs données personnelles.

Absence de coopération: la fraude à la carte est classée comme une infraction officielle que les autorités de poursuite pénale doivent poursuivre d'office. Un dépôt de plainte auprès de la police aide cette dernière dans ses enquêtes et dans la recherche de potentiels escrocs. Les délits cependant ne sont pas tous notifiés à la police, il s'en faut. Pour une infraction en ligne, la preuve est en outre plus difficile à établir qu'en cas de vol dans un magasin. L'identification des auteurs s'avère aussi bien souvent difficile. Notamment lorsque le fraudeur ou la personne lésée se trouvent dans un autre pays que le revendeur en ligne. D'où l'importance d'une coopération de toutes les parties concernées (titulaire de carte, émetteur, acquéreur, systèmes de cartes, autorités).

Aperçu des modes opératoires courants des escrocs

La migration croissante de la fraude par carte vers le e-commerce se révèle si l'on considère les tentatives de fraude les plus fréquemment commises:

Ingénierie sociale:

- **Hameçonnage (phishing)**: méthode consistant à se procurer de manière frauduleuse des informations privées. En règle générale l'escroc envoie un e-mail semblant à tous égards provenir d'une entreprise sérieuse, par exemple d'une banque ou d'une entreprise émettrice de cartes. Dans cet e-mail, l'expéditeur enjoint le destinataire de confirmer des informations et met en garde contre les conséquences qu'aurait la non-fourniture de telles informations. Cet e-mail peut aussi contenir un lien pointant vers un site aux apparences non suspectes et néanmoins frauduleux. Parmi les autres exemples figurent les annonces de paquets («Afin de pouvoir vous livrer le paquet…») ou les faux jeux-concours («Vous avez gagné…»).
- **Harponnage (spear-phishing):** le harponnage se distingue d'autres formes de hameçonnage en ce sens qu'il s'agit d'e-mails très personnalisés qui sont envoyés à des utilisateurs finaux sélectionnés. Pour avoir un effet plus convaincant, les fraudeurs procèdent préalablement à des recherches supplémentaires sur leurs victimes potentielles.
- **Hameçonnage vocal ou voice-phishing:** cette pratique est une tentative criminelle d'obtenir des informations privées, personnelles et financières par le biais de l'ingénierie sociale par téléphone.
- **Hameçonnage par SMS (SMS-phishing):** Cette pratique utilise des messages SMS pour tenter de persuader les victimes de divulguer des données personnelles ou confidentielles.

Data compromise (compromission des données; offres factices ou logiciels malveillants):

- **Fausses applis:** applis pour appareils portables incitant les utilisateurs à les télécharger et à les installer. Ces applis se présentent sous des formes réalistes et séduisantes, et proposent des services intéressants. Par contre, dès qu'elles sont installées sur un appareil mobile, elles peuvent causer un grand nombre de dommages.
- **Faux sites Web:** le but des site Web falsifiés est de pousser le client à divulguer des informations confidentielles, à télécharger des logiciels malveillants ou à acheter des produits qui ne seront jamais livrés.
- **Logiciels malveillants:** logiciel spécialement conçu pour perturber un système informatique, pour l'endommager ou pour accéder à ce système.

Autres modes opératoires connus

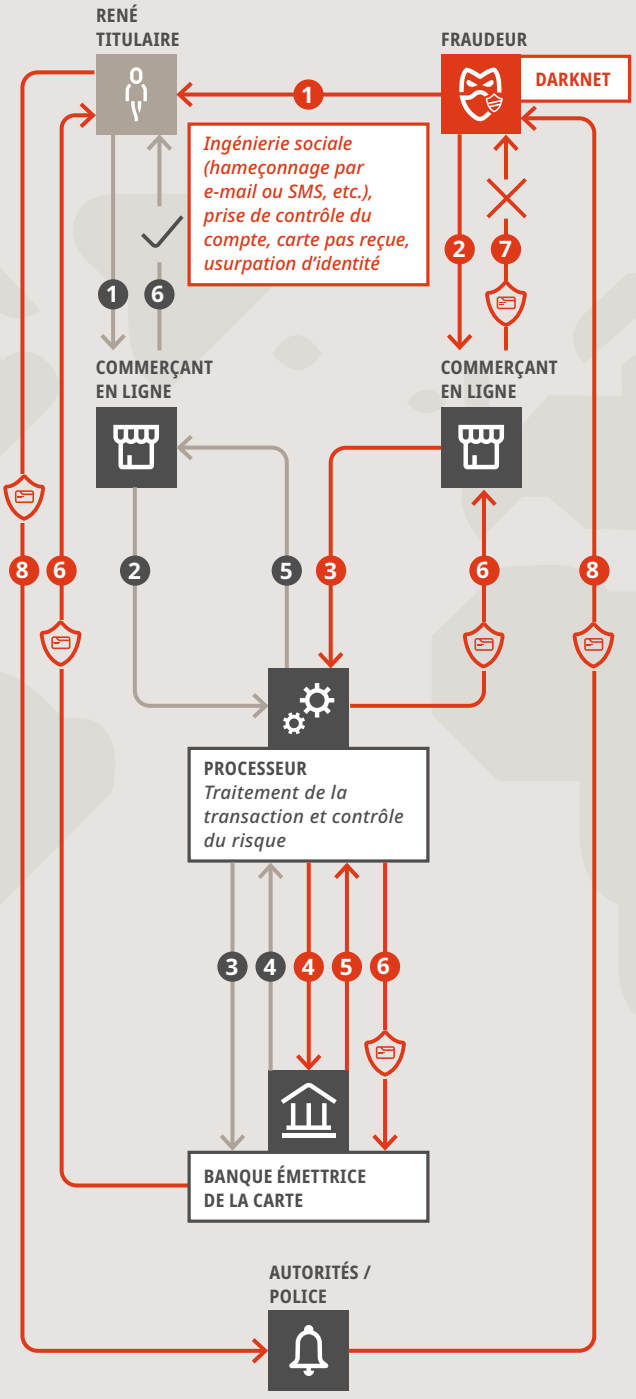
- **Écrémage ou e-skimming:** dans ce cas, c'est le processus de paiement des boutiques en ligne qui est infecté par un logiciel malveillant qui espionne les données de paiement et les données personnelles des clients durant le processus de paiement.
- **Attaque du numéro de la carte:** les escrocs utilisent les six à huit premiers chiffres d'une carte de paiement et calculent, à l'aide d'un logiciel, les chiffres restants possibles.
- **Détournement de compte (Account Hijacking):** il s'agit d'une forme d'usurpation d'identité dans laquelle les fraudeurs réussissent à accéder aux données de connexion d'un compte d'utilisateur.
- **Fraude au remboursement (également appelée «fraude à la rétrofacturation» – «Chargeback Fraud» – ou «Friendly Fraud»):** dans ce cas, un titulaire de carte prétend que ni lui ni une personne de son foyer n'a effectué d'achat en ligne ou qu'il n'a pas perçu les marchandises ou services achetés, afin de toucher le remboursement.
- **Schtroumpfage (Smurfing):** dans ce cas, les escrocs effectuent sur une période prolongée plusieurs petites transactions, afin de rester le plus longtemps possible sous les radars (méthode souvent employée aussi dans le blanchiment d'argent).
- **Vol de données:** des données sont soustraites d'un système sans que le propriétaire du système ne le sache ou sans qu'il ait donné son accord.
- **Usurpation d'identité (Spoofing):** ce mode opératoire consiste à camoufler une communication (p. ex. un e-mail, des appels téléphoniques) en provenance d'une source inconnue est techniquement déguisée, de sorte à faire croire qu'elle vient d'une source de confiance (expéditeur, numéro de téléphone).

Comment et où la fraude à la carte peut-elle se produire?

Dès lors que les escrocs sont en possession des données de la carte et éventuellement des mots de passe ou des codes PIN, une tentative de fraude pourrait se dérouler comme suit (transaction légitime – transaction abusive):

Transaction légitime par carte

1. René s'achète en ligne un nouveau téléphone mobile.
2. Via son processeur, le commerçant en ligne redirige la demande de transaction vers la procédure de contrôle. La demande d'autorisation traverse automatiquement le filtre des règlements enregistrés.
3. La demande d'autorisation est communiquée à la banque émettrice de la carte.
4. Après une vérification par la banque réussie, la validation est rétrosignalée au processeur.
5. Le processeur consolide les retours d'informations de la banque et des systèmes analysant les risques, puis il informe le commerçant que la transaction est validée.
6. L'achat peut être exécuté avec succès.



Transaction abusive par carte

1. L'escroc parvient à accéder aux données de carte et d'accès personnelles de René Titulaire.
2. L'escroc commande abusivement des marchandises sur Internet.
3. Via son processeur, le commerçant en ligne redirige la demande de transaction vers la procédure de contrôle. La demande d'autorisation traverse automatiquement le filtre des règlements enregistrés.
4. La demande d'autorisation est communiquée à la banque émettrice de la carte.
5. Après une vérification par la banque réussie, la validation est rétrosignalée au processeur.
6. Le processeur consolide les retours d'informations de la banque et des systèmes analysant les risques. La transaction est refusée à titre préventif, car le contrôle a fait ressortir un comportement d'achat inhabituel pour ce profil de carte.

   Suivant la définition de la règle, la carte peut en plus être temporairement bloquée. Dans l'outil de supervision, une alerte à la fraude est déclenchée, alerte que des analystes vérifient. La banque émettrice de la carte est informée de la transaction, elle contacte le titulaire de la carte en vue d'une analyse complémentaire du cas et pour se concerter sur la suite de la procédure.
7. Le commerçant en ligne refuse l'achat. La tentative d'escroquerie a été empêchée avec succès.
8. En déposant plainte, les titulaires de cartes aident la police dans ses enquêtes et dans la recherche de malfaiteurs et d'escrocs potentiels.

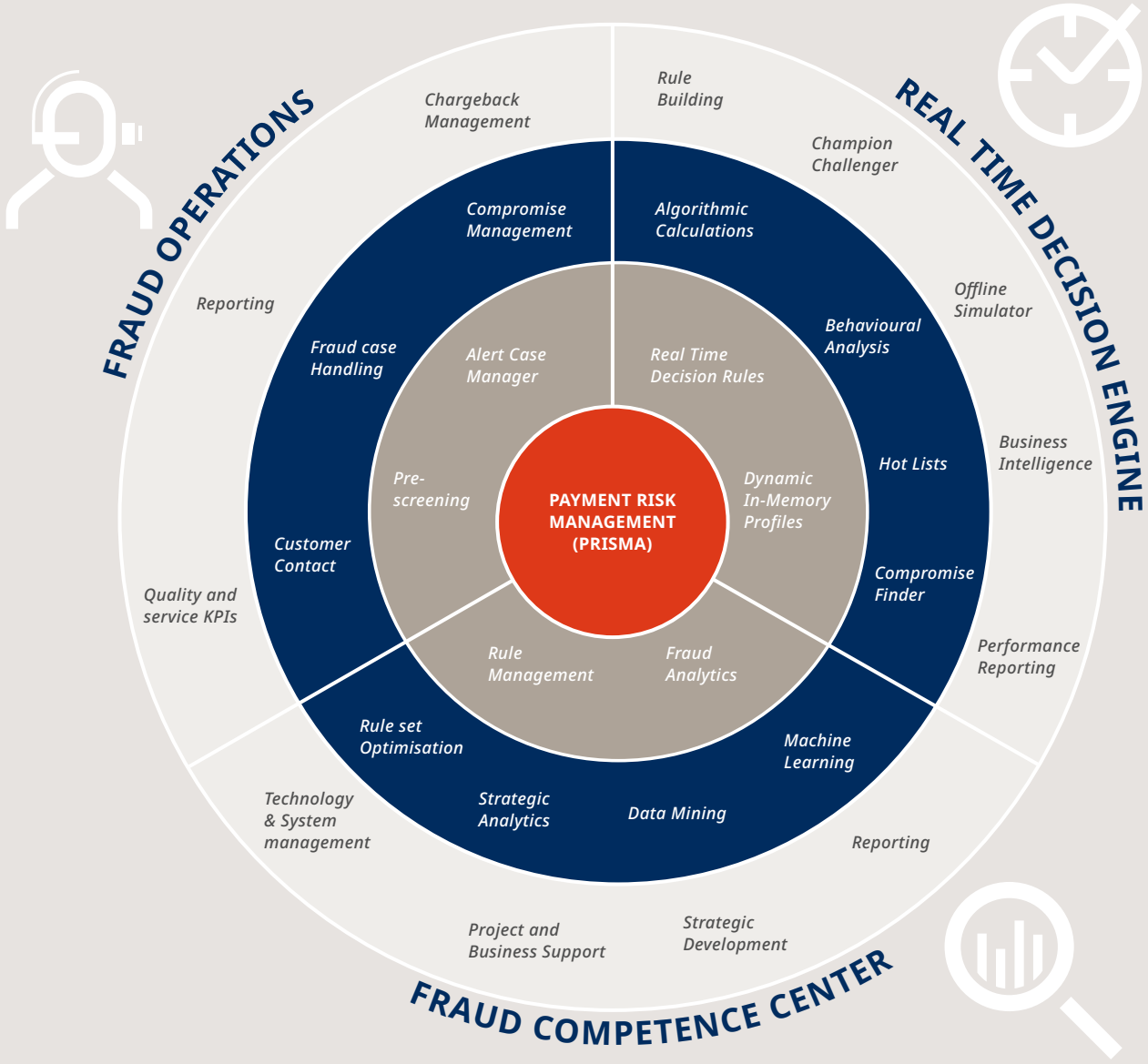
Comment lutter efficacement contre la fraude?

Les prestataires de services de paiements misent, dans la lutte contre la fraude, sur des systèmes en temps réel qui, grâce à l'emploi de technologies d'auto-apprentissage et à une gestion active des règles, réagissent de manière dynamique et rapide aux nouveaux mécanismes frauduleux.

Les experts antifraude (spécialistes scientifiques des données, administrateurs de règles et analystes des fraudes) peuvent détecter à court terme les tendances à la fraude émergentes et changeantes, et lutter contre de manière proactive. Ce travail consiste à optimiser constamment les règles utilisées permettant la reconnaissance des fraudes, afin de garantir le respect des exigences de sécurité les plus élevées.

En collaboration avec les équipes Fraud Operations qui officient comme une interface entre le Fraud Competence Center, les émetteurs de cartes (Issuers) et les systèmes de cartes, les titulaires de carte sont assurés d'être contactés de manière proactive en cas de transactions suspectes et de bénéficier d'une prise en charge optimale en cas d'utilisation frauduleuse confirmée de leur carte.

Illustration basée sur le modèle PRISMA (Payment Risk Management) utilisé par SIX.



Quelques mesures pour détecter et combattre avec succès la fraude à la carte

Titulaire de carte	Processeur/Issuer	
	Technique mise en œuvre:	Intelligence humaine: l'expertise des experts de la fraude
– Activation de 3DS (voir l'unité de formation 3D Secure) – Adapter les paramètres géographiques pour la région de mise en œuvre de la carte (géoblocage) – Fixation de montants limites pour la carte tels que des montants journaliers ou mensuels – Traitement confidentiel du numéro de carte et des mots de passe/codes PIN – Saine méfiance au moment d'ouvrir des e-mails ou des SMS ou d'y répondre (hameçonnage par mail ou SMS). Vérifier minutieusement l'expéditeur et passer le curseur de la souris sur les liens avant de cliquer – Achats effectués uniquement sur des sites dignes de confiance – Utilisation sur les différents sites Web de mots de passe divers et performants – Mise à jour régulière des logiciels et des appareils, c'est-à-dire qu'il faut toujours utiliser la dernière version du système d'exploitation, des applications, des scanners de virus, etc.) – Prudence lors d'appels (en cas de doute, composer directement le numéro de téléphone officiel)	**Utilisation de logiciels de pointe:** – Suivi en temps réel de toutes les autorisations de paiement – Supervision en temps quasi réel de tous les processus d'autorisation et de clearing – Profilage des historiques des transactions – Blocage automatisé des cartes – Rejet automatisé des transactions suspectes et abusives – Mise à jour régulière de l'ensemble des règles dans l'outil de supervision des fraudes (quotidiennement si nécessaire) en raison de nouveaux modèles de fraude et de nouvelles analyses (p. ex., cas de fraude non détectés) ou de conseils d'enquêteurs spécialisés dans la fraude (les nouvelles exigences du système de cartes peuvent également rendre des ajustements nécessaires) – Liste blanche/grise/noire – Échange intensif d'informations entre les parties concernées en cas d'incident (soupçon, abus, nouveaux systèmes de fraude) – Utilisation de la tokénisation pour crypter les informations de la carte (pour plus d'informations à ce sujet, voir l'unité de formation «Tokénisation pour les cartes de débit») – Examen via l'intelligence artificielle des transactions entrantes, en tenant compte des règles, des transactions abusives connues, des schémas comportementaux et de fraude avec des alertes en cas de divergences	**Analystes des fraudes:** – Examen de toutes les alarmes générées dans le système – Détection de nouveaux mécanismes frauduleux – Échange intensif d'expérience entre les experts de la fraude afin d'être constamment à jour – Analyse des points communs entre des cas de fraude similaires (p. ex. un CCP (Common Point of Purchase – point d'achat commun): à quel CPP la carte a-t-elle été compromise?), afin de détecter d'autres cas de fraude à la carte non encore signalés – Conseils pour adapter les règles – Échange intensif avec les banques participantes émettrices de cartes (Issuers) – Soutien des autorités en liaison avec l'usage abusif de cartes **Administrateurs de règles et scientifiques spécialiste des données:** – Analyse de nouvelles transactions abusives signalées – Analyse des conseils par des analystes antifraude – Simulation et test de nouvelles règles ou adaptations de règles – Analyses complexes en tenant compte de toutes les données disponibles – Établissement de statistiques/rapports – Création de modèles en liaison avec l'intelligence artificielle

CONCLUSION: LES CARTES DE DÉBITS SONT ET RESTENT SÛRES

La carte de débit est et reste un moyen de paiement très sûr. Grâce aux technologies les plus récentes, les moyens de paiement actuels (p. ex. sur terminal de magasin) s'accompagnent d'un taux de fraude extrêmement bas. Vu toutefois l'emploi des cartes dans le e-commerce, le thème de la fraude sans carte physique gagne de l'importance.

Les prestataires de services de paiements misent, dans la lutte contre la fraude, sur des systèmes en temps réel qui, grâce à l'emploi de technologies d'auto-apprentissage et à une gestion active des règles, réagissent de manière dynamique et rapide aux nouveaux mécanismes frauduleux.

Au cœur de la lutte réussie contre l'usage abusif des cartes: une interaction étroite entre la technique et le savoir-faire humain.

Grâce à des réseaux solides entre les prestataires de services de paiements et aux actions coordonnées avec des autorités telles qu'Europol et Interpol, il est régulièrement possible d'arrêter des gangs opérant à l'échelle internationale, de supprimer des places de marché sur le Darknet et d'arrêter les malfaiteurs.

La prévention offre la meilleure protection contre les escroqueries. SIX travaille depuis des années en étroite collaboration avec la police. Conjointement aux émetteurs de cartes, nous exploitons la plateforme de prévention card-security.ch qui, via différents canaux, informe les titulaires de cartes et le public sur le thème de la sécurité des cartes, et leur montre comment se protéger des utilisations frauduleuses.

SAVOIR PLUS

SIX BBS SA
Hardturmstrasse 201
Case postale
8021 Zurich
T +41 58 399 4012