feedzai

Comment les banques peuvent-elles protéger leurs clients contre l'escroquerie ?

Luis Junes

Avril 2024

C'est de plus en plus difficile de les arrêter

Instant Payments

augmentent les opportunités pour les criminels et nécessite une défense proactive

Escroqueries & Comptes mule

les criminels sont bien organisés et utilisent des technologies d'automatisation pour opérer à une échelle industrielle

Generative AI

permet aux criminels d'améliorer la qualité et la sophistication de leurs attaques

Les institutions financières investissent dans des solutions mais le problème ne ralentit pas

CHASE

"...each year we invest hundreds of millions of dollars in authentication, risk models, technology and associate/client education to make it harder for scammers to trick customers..."

News › North East News › Crime

Scammers posing as police officers tricked 'vulnerable' people into handing over £700,000

Los Angeles Times

BUSINESS

Column: Chase let an elderly customer wire more than $600,000 to an overseas scammer

Seine-et-Marne : 14 millions d'euros détournés grâce à une escroquerie au compte personnel de formation

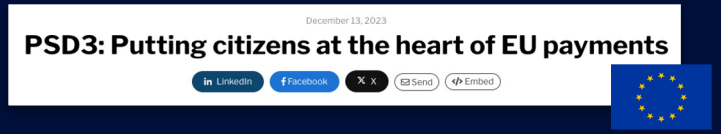
Una mujer de 73 años viaja a España para casarse con el cantante Luis Miguel y descubre que había vivido una estafa: "Yo lo veía venir pero no quería escuchar"

Responsabilité en cas d'escroquerie

Des pertes record poussent les régulateurs et les banques à prendre des mesures

Banks Plan to Start Reimbursing Some Victims of Zelle Scams

A rule change planned for early next year would shift liability for some losses onto the banks, not their customers.



December 13, 2023

PSD3: Putting citizens at the heart of EU payments

LinkedIn Facebook X Send Embed

Australian banks buckle to pressure over scams and vow to block transfers to suspect accounts

Consumer groups have long lobbied for institutions to crack down on scams by rejecting transfers if name and bank details of recipient don't match

Follow our Australia news live blog for latest updates

UK banks to reimburse fraud victims under new rules, regulator confirms

Requirement to refund people who have been tricked by scammers will be implemented in 2024

BC intensifica controle sobre indícios de fraudes

Compartilhe: Imprimir

Resolução estabelece regras para instituições compartilharem informações sobre indícios de irregularidades. Troca de dados deverá acontecer por meio eletrônico em até 24 horas contadas da identificação da tentativa de fraude. Medida detalha norma que já havia sido divulgada e que entra em vigor hoje, 1º de novembro.

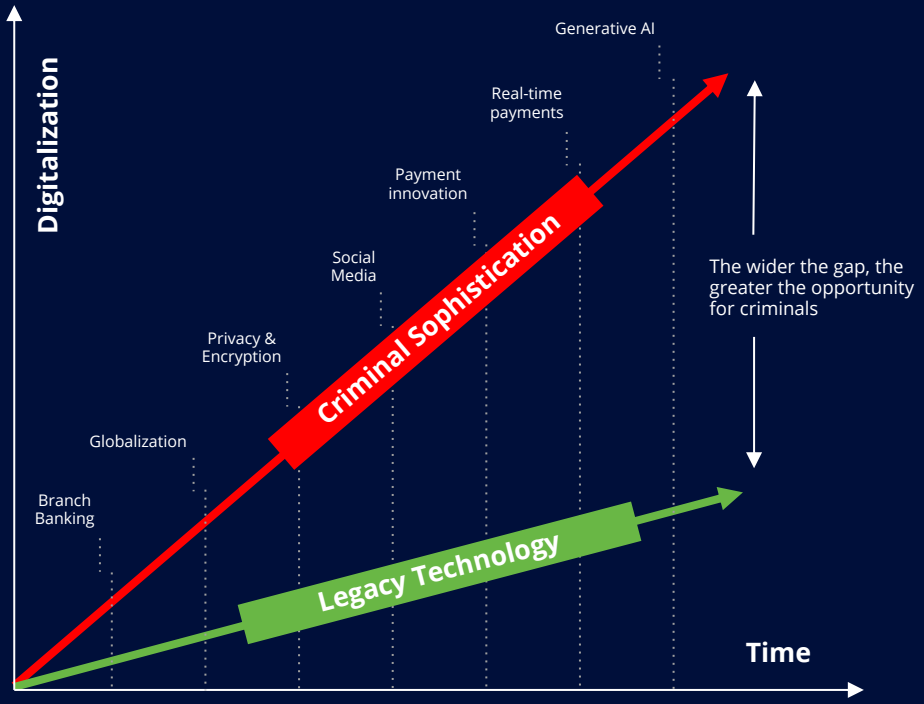
By Exception:
A 'no reimbursement' policy for scam victims, e.g. Australia, US*

Market Middle:
Case-by-case according to scam type, e.g. PSD3

Victim Friendly
100% on reimbursements, e.g. UK

Global Trend →

Les approches traditionnelles ne suivent pas le rythme



Silos de données

Les solutions traditionnelles “Legacy” ne partagent pas facilement les données et ne peuvent pas être utilisées dans d’autres applications de détection de fraude

Faible Performance

Les solutions existantes ne peuvent pas gérer les volumes de transactions actuels et font donc des compromis analytiques : cohortes, fenêtres d’anañyse courtes, mises à jour par lots, etc. Cela a un impact sur la capacité de détection en temps réel.

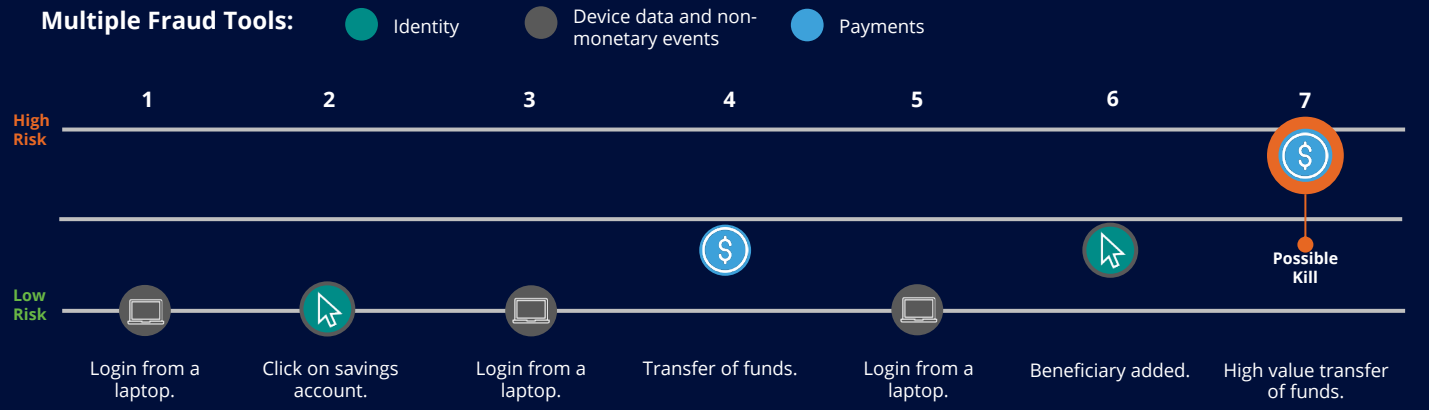
Faible Automatisation

Le recours à des règles et à des processus manuels plutôt qu’à l’IA signifie moins d’efficacité, plus de coûts humains et plus d’erreurs.

Il est essentiel de connecter les données tout au long du cycle de vie

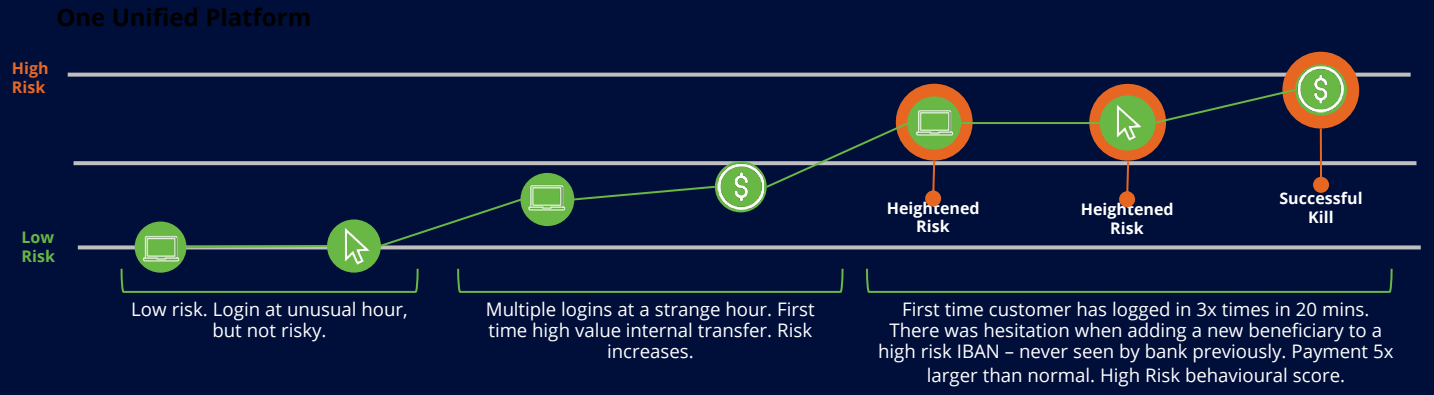
Suboptimal Approach

Les approches traditionnelles fonctionnent en silos et ne peuvent pas évaluer les risques dans leur contexte. La détection précoce et la réponse sont difficiles.



Best in Class Approach

L'analyse en temps réel du comportement, des appareils et des transactions permet une détection précoce et renforce les points de blocage



Multiples couches fournissent une valeur incrémentielle

Response Completeness

Capability	Scam Prevention solution component	Strategy effectiveness
Risk Engine	**Customer Profiling** (age, tenure etc)	
Risk Engine	**AI Based Transactional Profiling** (user level, value, beneficiary focus)	
Risk Engine	**Multi Event Profiling** (adding non-monetary and other channels)	
Risk Engine	**Inbound Payment Profiling** (mule detection)	
Enrichment	**Behavioral Biometrics** (RAT, active call, hesitation)	
Risk Engine	**Scam Trained Models** (based on known scam labels)	
Case Manager	**Operational Excellence** (scam specific queues)	
Risk Engine	**Data Led Education** (in journey, MO categorization)	
Enrichment	**Network Scoring** (globally applied data learnings)	

Une approche holistique et multidisciplinaire pour réduire les escroqueries

1. Institutions Financières

Moderniser les systèmes de détection en temps réel pour inclure du Machine Learning et davantage de données contextuelles

2. Opérateur Mobiles

Partager des informations qui pourraient être utilisées pour déterminer une activité suspecte et la signaler

3. Réseaux Sociaux

Établir des contrôles plus stricts pour la création d'utilisateurs et la détection de comportements suspects

4. Régulateurs

Continuer à adopter une réglementation pour protéger les consommateurs contre les escroqueries.

5. Éducation et Sensibilisation

Programmes de sensibilisation à l'intention des consommateurs et du grand public

Merci

feedzai