CLUBBANQUE

Par Revue Banque

Fraude aux paiements

15 mai 2025

feedzai

Partenaire de l'événement

Square management

Partenaire officiel

CLUB
BANQUE

Jean-François Filliatre
Direction éditoriale
Revue Banque

Programme

Fraude aux paiements

Introduction
Michèle Hallak, directrice France, Feedzai

Keynote : Cadre règlementaire
Daniel Labaronne, membre de la Commission des Finances et auteur de la récente proposition de loi sur contre les fraudes aux moyens de paiement scripturaux, Assemblée Nationale

---

Table Ronde
Animation : Jean-François Filliatre, direction éditoriale, Revue Banque
Daniel Labaronne, membre de la Commission des Finances, Assemblée Nationale
Jérôme Raguénès, directeur du département numérique, paiements et résilience opérationnelle, FBF
Questions / Réponses

Keynote : Fraude : l'évolution de la jurisprudence
Pierre Storrer, avocat au barreau de Paris, Storrer et associés

---

Table Ronde : Aspects opérationnels et technologiques
Animation: Michèle Hallak, directrice France, Feedzai
Luis Junes, expert en prévention de la fraude, Feedzai
Julien Goulian, responsable du Département de Prévention et de Lutte Contre la Fraude, BNP Paribas
Samuel Willy, responsable Data & Lutte contre la Fraude, Cartes Bancaires
Questions / Réponses

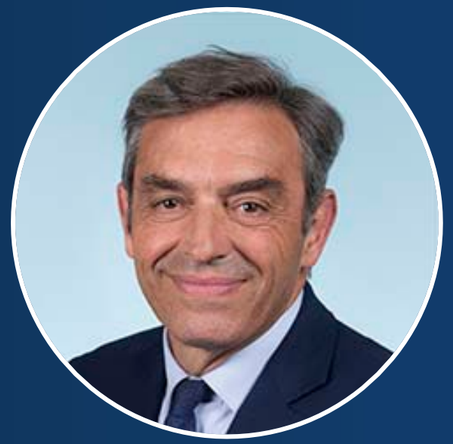
Cocktail

CLUB BANQUE

CLUB BANQUE

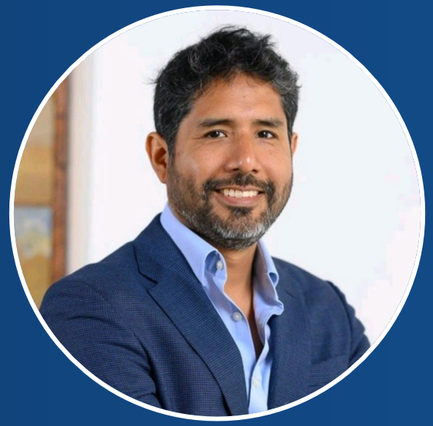
Les intervenants

feedzai



Daniel Labaronne
Membre de la Commission des Finances
Assemblée Nationale

Michèle Hallak
Directrice France
Feedzai



Luis Junes
Expert en prévention de la fraude
Feedzai

Julien Goulian
Responsable du Département de Prévention et de Lutte Contre la Fraude
BNP Paribas

CLUB BANQUE

Les intervenants

feedzai

Jérôme Raguénès
Directeur du département Numérique,
Paiements et Résilience opérationnelle
FBF

Pierre Storrer
Avocat au barreau de Paris
Storrer et associés

Samuel Willy
Responsable Data & Lutte
contre la Fraude
Cartes Bancaires

CLUB
BANQUE

Michèle Hallak
Directrice France
Feedzai

A propos de Feedzai- l'IA de confiance

Les clients du monde entier font confiance à Feedzai

Notre mission

Nous protégeons les paiements et créons de la confiance client avec nos solutions natives de l'IA qui stoppent la fraude et rendent la conformité AML plus efficace

A propos de nous

- Fondée en **2011**
- **11** bureaux sur **4** continents
- **~600** employés en croissance

Leader du secteur

IDC
Best in Class Integrated FinCrime Platform

Chartis
Category Leader in Payment Risk Solutions

datos INSIGHTS
Best in Class Fraud and AML Vendor

feedzai

~1 milliard
Clients protégés dans le monde

>$8 mille milliards
de paiements processés par an

>70 milliards
d'évènements traités par an

feedzai RiskOps Platform, IA de confiance

feedzai

AGENTS IA

ScamAlert
Multimodal GenAI model that detects scam attempts such as Purchase, Invoice & CEO

Behavioral Score
Fraudulent session score based on behavioral and device intel

Case Summary Agent
Feedzai GenAI Case Summaries with purpose-built visualization

SAR Agent
Creates and populates SAR filings with case information and narrative

PRODUITS RISKOPS

AI ORCHESTRATION ENGINE

Identity

Fraud

AML

PLATEFORME IA

Foundational AI & Machine Learning Models

Responsible AI Training & Runtime Platform

FEEDZAI IQ™

Feedzai TrustScore
Federated Learning risk score made out of the insights and patterns from Feedzai's global footprint

Feedzai TrustSignals
Proprietary Feedzai enrichment data providing risk prevalence on many facets of a transaction

DATA CLIENTS

Monetary Data
Cards, Transfers, P2P, RTP, ACH, Wires, SEPA, etc

Non Monetary Data
Customer Demographics, Account Changes, Logins, etc

SDKs PROPRIETAIRES

Behavioral Collectors
Accelerator, Active Call, Swipe Patterns, Keystrokes, etc

Device Collectors
Device ID, Color Depth, Screen Resolution, OS & Browser, IMEI, etc

Network Collectors
IP, Domain, VPN, WiFi SSID/BSSID, ASN, Country, City, etc

FEEDZAI RISKOPS PLATFORM

Les solutions de Feedzai protègent tout le parcours client

Une plateforme de bout-en-bout, identité, fraude, AML

Parcours client

Enrôlement & Onboarding | Authentification | Transactions de paiement | Changements de device et compte

Feedzai Solutions

Identity

- Orchestration
- Account Opening
- New Account Fraud
- Account Monitoring

Fraud

- Transaction Fraud
- Scam Prevention
- Risk Management for Acquirers

AML

- KYC / CDD
- Watchlist Screening
- AML Transaction Monitoring

Chartis RiskTech AI50 2024 — **Top AI-Driven Platform**

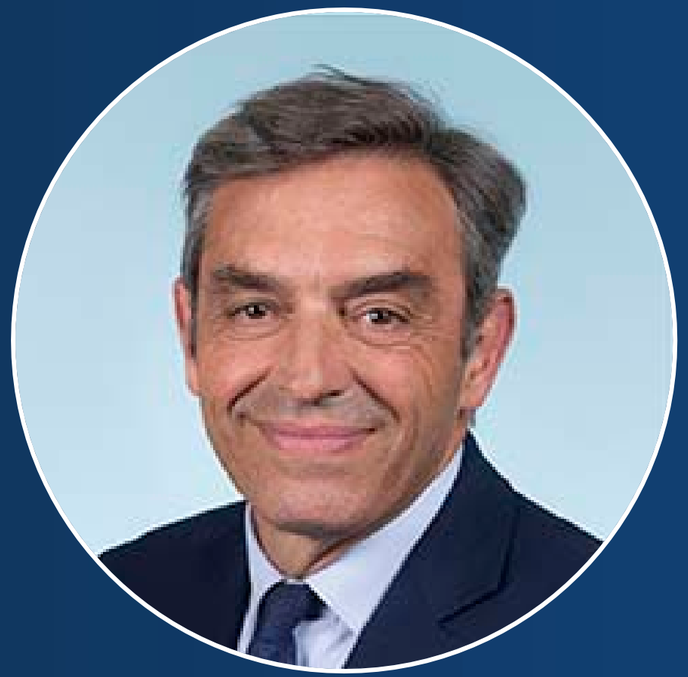
Le seul leader mondial reconnu dans les trois domaines

datos INSIGHTS

IDC

Liminal

CLUB
BANQUE

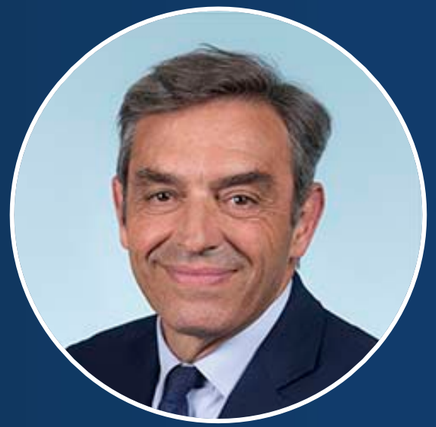


Daniel Labaronne
Membre de la Commission des Finances
Auteur de la récente proposition de loi
sur contre les fraudes aux moyens
de paiements scripturaux
Assemblée Nationale

CLUB BANQUE

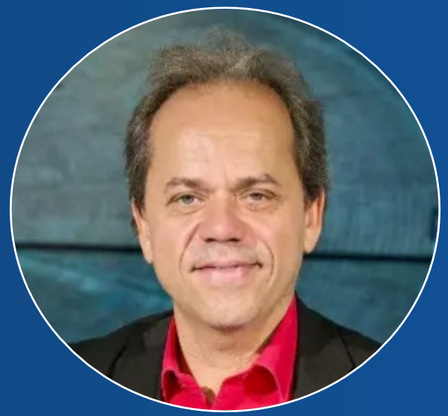
Table ronde

feedzai



Daniel Labaronne
Membre de la Commission des Finances
Assemblée Nationale

Jérôme Raguénès
Directeur du département
Numérique, Paiements et
Résilience opérationnelle
FBF



Jean-François Filliatre
Direction éditoriale
Revue Banque

CLUB
BANQUE

feedzai

Questions / Réponses

CLUB
BANQUE

Pierre Storrer
Avocat au barreau de Paris
Storrer et associés

1. Textes

- DSP 1 et 2, et proposition de RSP
- CMF, art. L. 133-1 et s.
- C. civ., art. 1231-1

2. Jurisprudence

2.1 CJUE

- CJUE, 2 sept. 2021, aff. C-337/20, CRCAM (*exclusivité du régime spécial de responsabilité pour les opérations de paiement non autorisées ou mal exécutées*)
- CJUE, 16 mars 2023, aff. C-351/21, Beobank (*qualification préalable d'opérations de paiement autorisées ou non*)
- CJUE, 11 juill. 2024, aff. C-409/22, Eurobank Bulgaria (*consentement à l'exécution d'une opération de paiement – preuve par le PSP*)

2.2 Cour de cassation

- Cass. com., 1er juin 2023, n° 21-19.289, Bull. civ. IV, p. 85, Lettre chambre commerciale n° 10, juill. 2023, p. 8 (*opérations de paiement non autorisées – modification ultérieure de l'IBAN du bénéficiaire – consentement au bénéficiaire de l'opération de paiement*)
- Cass. com., 30 août 2023, n° 22-11.707, Bull. civ. IV, p. 7 (*opérations de paiement non autorisées – absence d'authentification forte – décharge du payeur sauf agissement frauduleux de sa part*)
- Cass. com., 14 févr. 2024, n° 22-11.654, Bull. civ. IV, p. 68 (*virements frauduleux libellés en USD – régime de responsabilité contractuelle de droit commun*)
- Cass. com., 27 mars 2024, n° 22-21.200, Bull. civ. IV, p. 67, Lettre chambre commerciale n° 13, juill. 2024, p. 8 (*opérations de paiement non autorisées – exclusivité du régime spécial de responsabilité*)
- Cass. com., 2 mai 2024, n° 22-17.233, Bull. civ. IV, p. 86, Lettre chambre commerciale n° 13, juill. 2024, p. 9 (*ordres de paiement donnés oralement – opération de paiement autorisée – régime de responsabilité contractuelle de droit commun*)
- Cass. com., 2 mai 2024, n° 22-18.074, Bull. civ. IV, p. 90 (*retraits et paiements effectués par une épouse à l'aide du doublon d'une carte bancaire de son conjoint obtenu à son insu – opérations de paiement non autorisées – régime spécial de responsabilité*)
- Cass. com., 2 oct. 2024, n° 23-13.282, Bull. civ. IV, p. 62, Lettre chambre commerciale n° 14, nov. 2024, p. 9 (*fraude au président – virements au profit d'un compte hors zone SEPA – régime de responsabilité contractuelle de droit commun*)
- Cass. com., 23 oct. 2024, n° 23-16.267, Bull. civ. IV, p. 60, Lettre chambre commerciale n° 14, nov. 2024, p. 10 (*fraude au conseiller bancaire par* spoofing – *absence de négligence grave du payeur*)
- Cass. com., 20 nov. 2024, n° 23-15.099, Bull. civ. IV, p. 83 (*vol des instruments de paiement – absence de négligence grave du payeur faute de recherche préalable par le PSP que les opérations non autorisées ont été authentifiées, dûment enregistrées et comptabilisées, et qu'elles n'ont pas été affectées par une déficience technique ou autre*)
- Cass. com., 15 janv. 2025, n° 23-13.579, Bull. civ. IV, p. 69, Lettre chambre commerciale n° 15, mars 2025, p. 8 (*la négligence grave du payeur exclut un partage de responsabilité avec la banque*)
- Cass. com, 15 janv. 2025, n° 23-15.437, Bull. civ. IV, p. 72, Lettre chambre commerciale n° 15, mars 2025, p. 8 (*virement frauduleux exécuté conformément à l'identifiant unique du bénéficiaire – absence de responsabilité de droit commun de la banque*)
- Cass. com., 30 avr. 2025, n° 24-10.149, publié au Bull. (*ajout frauduleux de bénéficiaire de virement – preuve préalable par le PSP que l'opération de paiement a été authentifiée, dûment enregistrée et comptabilisée, et qu'elle n'a pas été affectée par une déficience technique ou autre*)

3. Autres

- Orientations modifiées EBA/GL/2018/05 concernant les exigences pour la déclaration de données relatives à la fraude au titre de l'article 96, § 6, de la DSP 2
- Rapports OSMP
- Recommandations OSMP sur les modalités de remboursement des opérations de paiement frauduleuses, 16 mai 2023, Rapport OSMP 2022, p. 27

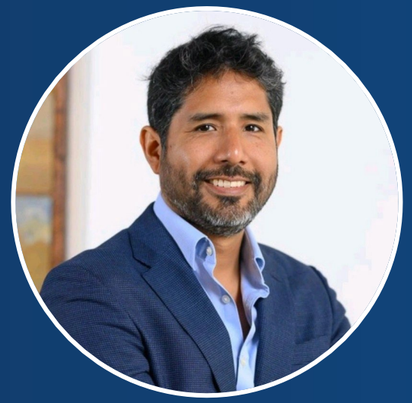
CLUB BANQUE

feedzai

Table ronde

Aspects opérationnels et technologiques

Michèle Hallak
Directrice France
Feedzai



Luis Junes
Expert en prévention
de la fraude
Feedzai

Julien Goulian
Responsable du Département
de Prévention et de Lutte
Contre la Fraude
BNP Paribas

Samuel Willy
Responsable Data &
Lutte contre la Fraude
Cartes Bancaires

CLUB
BANQUE

feedzai

Questions / Réponses

Avenir

CLUB BANQUE

Les prochains événements

CLUB BANQUE

Information extra-financière : premières leçons pratiques de l'application de la CSRD

12 juin 2025

La mise en œuvre opérationnelle du paquet européen LAB/FT

3 juillet 2025

RB LIVE

Décrochage économique et financier de l'Europe : Quelle réalité ? Comment rebondir ?

11 juin 2025

DÉBATS REVUE BANQUE

Modèles de crédit-Portefeuilles CIB -
Nouveaux risques et nouvelles stratégies dans un Monde en pleine mutation

24 juin 2025

Inscription et renseignements : evenements@revue-banque.fr 01.48.00.54.04

Profitez du Club Banque toute l'année avec l'adhésion !

Inscription et renseignements :

clubbanque@revue-banque.fr

01.48.00.54.04

CLUB BANQUE

REVUE BANQUE

« CLUB BANQUE » du 15 mai 2025

Fraude aux paiements

Introduction
Michèle Hallak, directrice France, Feedzai

Keynote : Cadre réglementaire
Daniel Labaronne, membre de la Commission des Finances et auteur de la récente proposition de loi sur contre les fraudes aux moyens de paiement scripturaux, Assemblée nationale

Table Ronde
Daniel Labaronne
Jérôme Raguénès, directeur du département numérique, paiements et résilience opérationnelle, FBF

Questions / Réponses

Keynote : Fraude : l'évolution de la jurisprudence
Pierre Storrer, avocat au barreau de Paris, Storrer et associés

Table Ronde : Aspects opérationnels et technologiques
Jean-François Filliatre, direction éditoriale, Revue Banque
Michèle Hallak, directrice France, Feedzai
Luis Junes, expert en prévention de la fraude, Feedzai
Julien Goulian, responsable du Département de Prévention et de Lutte Contre la Fraude, BNP Paribas Banque Commerciale en France
Samuel Willy, Responsable Data & Lutte contre la Fraude, Cartes Bancaires

Questions / Réponses

Introduction

Jean-François FILLIATRE, direction éditoriale, Revue Banque

Bonjour et bienvenue à ce cinquième Club Banque de l'année, en partenariat avec Square Asset Management. Ce rendez-vous mensuel explore une thématique différente, avec envoi des présentations dès le lendemain et des possibilités d'échanges pendant la session et lors du cocktail.

En juin, nous parlerons des premiers rapports de CSRD avec peut-être un point sur la directive Omnibus, en juillet de la lutte contre le blanchiment, et en septembre du dossier Dora.

Ce soir, nous aborderons le thème de la fraude avec Feedzai.

Nous accueillons :

- Michèle Hallak, directrice France de Feedzai ;
- Daniel Labaronne, membre de la Commission des Finances et auteur de la récente proposition de loi sur contre les fraudes aux moyens de paiement scripturaux, Assemblée nationale ;
- Jérôme Raguénès, directeur du Département numérique, paiements et résilience opérationnelle, FBF ;
- Luis Junes, expert en prévention de la fraude, Feedzai ;
- Julien Goulian, responsable du Département de prévention et de lutte contre la fraude, BNP Paribas Banque Commerciale en France ;
- Jérôme Raguénès, directeur du Département numérique, paiements et résilience opérationnelle, FBF ;
- Pierre Storrer, avocat et contributeur régulier de Banque et Droit, spécialisé dans les moyens de paiement ;
- Samuel Willy, Responsable Data & Lutte contre la Fraude, Cartes Bancaires.

Notre programme se déroulera en deux parties : d'abord les aspects juridiques et réglementaires avec Daniel Labaronne sur sa proposition de loi, suivi d'un débat avec Jérôme Raguénès et d'un point jurisprudentiel par Pierre Storrer ; ensuite, une table ronde animée par Michèle Hallak sur l'évolution de la fraude, les solutions et l'impact de l'intelligence artificielle.

Michèle HALLAK, directrice France de Feedzai

Feedzai est spécialisée dans la lutte contre la fraude au paiement, un sujet crucial qui préoccupe utilisateurs, établissements bancaires, institutions financières et régulateurs.

Créée en 2011 au Portugal par trois ingénieurs de l'Agence spatiale européenne, Feedzai a développé des algorithmes d'intelligence artificielle initialement conçus pour les navettes spatiales, adaptés ensuite au secteur des paiements. Notre premier client était First Data, aujourd'hui Fiserv.

Nous sommes devenus l'un des leaders mondiaux de la lutte contre la fraude au paiement et la criminalité financière, protégeant plus d'un milliard de clients finaux à travers le monde. Nous sécurisons 8 000 milliards de dollars de transactions, proches des 9 000 milliards de MasterCard. Notre société compte 600 employés répartis sur 11 bureaux.

L'intelligence artificielle est au cœur de notre plateforme. Nous développons une IA de confiance, non biaisée et explicative - pas une « black box ». Ce point est crucial pour les institutions bancaires et financières qui peuvent ainsi comprendre et justifier les décisions de rejet d'opérations ou d'identification de risques de fraude.

Notre système collecte des données via des SDKs sur les applications mobiles des banques et des données bancaires pour créer un profil granulaire de chaque client individuel, contrairement aux systèmes traditionnels qui fonctionnent par segments.

Notre système détermine le comportement normal d'un utilisateur pour détecter précisément toute déviation qui pourrait signaler une fraude, réduisant ainsi considérablement les faux positifs. Nous privilégions le *machine learning* par rapport aux règles traditionnelles. Notre innovation Feedzai IQ permet aux banques d'implémenter des modèles de *machine learning* dès le premier jour en utilisant l'intelligence de notre réseau sans partager les données. Ces modèles s'améliorent avec le temps. Nous utilisons également l'IA générative avec ScamAlert pour protéger les clients contre les arnaques et automatiser les rapports SAR. Notre solution offre aux banques une vision unique de chaque client tout au long de son parcours, détectant même des comportements inhabituels comme une utilisation différente de la souris sous stress, permettant une intervention en temps réel.

Keynote : Cadre réglementaire

Daniel LABARONNE, membre de la Commission des Finances et auteur de la récente proposition de loi sur contre les fraudes aux moyens de paiement scripturaux, Assemblée nationale

La fraude bancaire représente 1,2 milliard d'euros et touche les entreprises, les particuliers et les administrations. Concernant les chèques, nous voyons des fraudes impliquant des « mules » qui déposent des chèques volés sans le savoir, créant des situations dramatiques lorsqu'on leur demande de rembourser. Pour les IBAN, des *hackers* interceptent des communications commerciales légitimes et modifient les coordonnées bancaires pour détourner les paiements. La Cour de cassation a récemment dédouané les banques de toute responsabilité dans ces cas.

Ma proposition de loi, élaborée avec l'écosystème bancaire et les associations de consommateurs, vise à protéger tous les acteurs, y compris les banques. Elle s'inscrit dans une démarche politique plus large, portée par Ensemble pour la République, de lutte contre toutes les fraudes - fiscale, sociale et douanière - qui représentent environ 20 milliards d'euros notifiés en 2023, dont 13 milliards récupérés.

Cette proposition s'aligne avec les initiatives européennes comme la DSP2, qui a introduit l'authentification forte sur un certain nombre de paiements, et anticipe le futur règlement DSP3 qui prévoit un contrôle de concordance entre l'IBAN et l'identité du bénéficiaire.

Concrètement, nous créons un fichier des IBAN frauduleux alimenté par les banques, géré par la Banque de France et contrôlé par la CNIL. Ce système permettra le partage d'informations entre tous les opérateurs bancaires pour identifier les IBAN frauduleux. Bien que la fraude à l'IBAN ne représente « que » 300 millions d'euros, c'est considérable pour les victimes.

Une attention particulière a été portée à la vérification avant de qualifier un IBAN de frauduleux. Pendant cette phase d'examen, les opérations bancaires ne sont pas immédiatement bloquées. Avec les députés, nous avons convenu que pendant cette phase d'analyse qui peut durer quelques jours, les comptes ne sont pas bloqués, mais dès que l'IBAN est confirmé frauduleux, le compte est bloqué.

La PPL adoptée au Sénat et à l'Assemblée sur la fermeture abusive des comptes bancaires contient une absurdité : elle prévoit que le titulaire d'un compte clôturé doit être informé immédiatement, sauf s'il s'agit d'un escroc. Paradoxalement, si vous n'êtes pas informé de la fermeture, vous savez que vous êtes considéré comme escroc !

Ma proposition de loi comporte trois articles principaux. Le premier crée un fichier d'IBAN frauduleux. Le deuxième renforce le cadre juridique contre la fraude au chèque en élargissant le fichier national des chèques irréguliers pour inclure non seulement les faux chèques mais aussi les chèques falsifiés et contrefaits. Le troisième permet aux banques de consulter ce fichier avant de payer un chèque, pour éviter notamment le mécanisme de « mule ».

Cette PPL a été adoptée à l'unanimité car elle est très technique, sans fondement politique sous-jacent, et nous avons travaillé avec toutes les parties prenantes. J'ai écarté certaines propositions hors sujet comme celles concernant les cartes bleues, la PPL se concentrant uniquement sur les IBAN et les chèques. Le texte est maintenant au Sénat et j'espère qu'il ne sera pas dénaturé.

Table ronde

Jean-François FILLIATRE

Avons-nous une idée du calendrier d'examen de votre texte ?

Daniel LABARONNE

Nous n'avons pas de calendrier précis, mais nous faisons tout pour que le texte soit examiné avant la fin de la session parlementaire fin juin. Il y a beaucoup de pression, de tous côtés : Bercy, la Fédération bancaire française, la Banque de France. Pour faire avancer une PPL, il faut d'abord convaincre son groupe politique que c'est prioritaire.

Jean-François FILLIATRE

Gabriel Attal a été facile à convaincre ?

Daniel LABARONNE

Oui, car il a compris que mon projet s'inscrivait dans notre action générale contre les fraudes. Il n'avait pas pensé à la fraude bancaire spécifiquement. Une fois qu'il a vu que c'était une brique supplémentaire dans notre démarche politique, cela a été plus facile.

Jean-François FILLIATRE

Quel est le rôle des banques dans la lutte contre la fraude ?

Jérôme RAGUÉNÈS, directeur du département Numérique, Paiements et Résilience opérationnelle de la FBF

C'est une lutte constante. Comme l'a expliqué M. Labaronne, la fraude sur les paiements représente 1,2 milliard d'euros. Il s'agit du lien de confiance entre la banque et le client, dans les paiements quotidiens, de proximité et sur Internet. La fraude évolue constamment, c'est le jeu du gendarme et du voleur. Nous avons les outils techniques mais nous sommes contraints par la réglementation. Actuellement, une banque qui identifie un IBAN frauduleux ne peut pas communiquer cette information aux autres établissements. Nous avons fait des pilotes avec la Banque de France qui ont montré que ce partage d'information permettrait d'être plus réactif et de protéger davantage de clients.

Jean-François FILLIATRE

Commençons par l'article 2. Vous êtes-vous interrogé sur le coût du dispositif concernant le chèque ?

Daniel LABARONNE

Il n'y aura pas de facturation pour alimenter le fichier national des chèques irréguliers, mais il pourra y avoir une facturation pour sa consultation. C'est le modèle économique retenu, similaire à ce qui existe depuis 30 ans. L'objectif était de consolider juridiquement cet outil existant et de l'étendre à d'autres types de fraudes aux chèques.

Jean-François FILLIATRE

Quelle est votre réaction sur le texte tel qu'il existe aujourd'hui ?

Jérôme RAGUÉNÈS

Ce dispositif complète notre arsenal et permettra aux banques d'effectuer des contrôles supplémentaires. Le chèque est un moyen de paiement papier qui ne peut pas offrir le même niveau de sécurité qu'une carte bancaire ou les nouveaux modes de paiement. Cette faiblesse inhérente nous oblige à trouver des parades. Au-delà de l'interrogation du fichier, nous travaillons sur d'autres problèmes comme la fraude à la « mule » et le vol des carnets de chèques avant leur remise au client. La profession bancaire développe des propositions pour renforcer la sécurité et compliquer le travail des fraudeurs.

Jean-François FILLIATRE

Avez-vous eu des débats au sein de la Commission des finances ou de l'Assemblée nationale concernant le chèque ? Est-ce que la question de sa pertinence comme

moyen de paiement en France a été discutée, notamment dans le cadre de la réglementation contre les chèques volés ?

Daniel LABARONNE

Il n'y a pas eu beaucoup de débats sur cette question. Nous n'avons pas abordé l'alternative chèque payant *versus* chèque gratuit. La proposition de loi est un objet extrêmement technique, ce qui limite les angles de critique. Le débat est resté technique, avec le soutien de députés connaissant l'activité bancaire, y compris un député de Touraine d'un autre bord politique ayant longtemps travaillé à la Banque de France. En résumé, il n'y a pas eu de débat sur l'utilisation, la suppression ou la tarification du chèque.

Jean-François FILLIATRE

Le texte est-il parfaitement adapté aux problématiques de fraude à l'IBAN, même si le poids de cette fraude reste relativement limité ?

Jérôme RAGUÉNÈS

La fraude au virement représente environ 300 millions. Le partage d'IBAN frauduleux permet de réduire cette fraude de 6 à 10 %, soit près de 30 millions d'euros et des dizaines de milliers de clients protégés. L'important dans ce dispositif est que la loi permet aux banques et prestataires de services de paiement d'échanger des données, aujourd'hui l'IBAN car c'est la donnée la plus pertinente. La plateforme mise en place pourra évoluer pour intégrer d'autres données à l'avenir. C'est une course entre gendarmes et voleurs : quand les fraudeurs s'adapteront, la fraude se déplacera vers d'autres solutions, et nous devrons nous adapter également

Jean-François FILLIATRE

Comment réagissez-vous à l'idée que ce système centralisé par la Banque de France avec le contrôle de la CNIL pourrait à l'avenir être étendu à d'autres types de données comme des adresses IP ou des adresses mail de fraudeurs ?

Daniel LABARONNE

Toute évolution devra respecter le RGPD puisque c'est contrôlé par la CNIL. Si c'est le cas, des évolutions sont envisageables. Sinon, nous devrons légiférer à nouveau pour inventer des dispositifs adaptés. C'est un travail permanent car les fraudeurs ont une imagination très fertile. Je rappelle également que tout ne repose pas sur le législatif : des dispositifs réglementaires peuvent être introduits par les autorités monétaires ou le gouvernement.

De la salle

Pour les chèques falsifiés et irréguliers, on ne le sait qu'après leur circulation et leur rejet, donc je ne vois pas l'intérêt de consulter ce fichier. En revanche, pour les chéquiers volés, c'est très utile car le chèque en circulation ne sera pas payé. Cette disposition était attendue depuis longtemps - les commerçants pouvaient interroger le fichier des chéquiers volés mais pas les banques, ce qui est aberrant. Consulter ce fichier pendant la circulation du chèque protégerait mieux les clients.

Jérôme RAGUÉNÈS

Nous avons un accès à ce fichier. Sur les chéquiers volés, beaucoup le sont avant d'arriver au titulaire du compte. Nous travaillons avec la profession pour sécuriser l'envoi des chéquiers aux clients. Il faut respecter le choix du client : venir en agence, envoi par courrier simple ou recommandé. Au-delà, nous réfléchissons à des mécanismes de sécurité comme informer le client de l'envoi de son chéquier afin qu'il puisse signaler la non-réception après dix jours, permettant d'enregistrer le chéquier comme volé. Nous travaillons sur l'ensemble du cycle de vie du produit et espérons faire des propositions prochainement.

De la salle

Qu'en est-il des IBAN éphémères, virtuels qui disparaissent dans le temps et peuvent être associés à un IBAN source, dont la banque émettrice n'a pas forcément connaissance ? Comment la loi prévoit-elle d'intégrer ces innovations liées aux fintechs comme WISE ?

Daniel LABARONNE

La proposition de loi intègre ces nouveaux vecteurs de paiement ou de virement, car on avait attiré mon attention sur ces outils. Je rappelle que la création d'un fichier nécessite une autorisation par la loi, qui doit respecter le RGPD. Il faut également définir qui a le droit de consulter ce fichier et l'encadrer d'un point de vue réglementaire. C'est exactement ce que j'ai proposé dans cette loi.

De la salle

Je suis médiateur auprès de l'ASF et très intéressé par votre proposition car nous avons beaucoup de saisines liées aux fraudes utilisant de vrais IBAN frauduleux. Quand ce mécanisme sera-t-il effectif ? Quelle sera la nature de l'obligation de déclaration quand une banque identifiera un IBAN frauduleux ? Les banques seront-elles obligées de consulter ce fichier à chaque ajout d'un nouveau bénéficiaire ?

Jérôme RAGUÉNÈS

Nous travaillons sur ce sujet depuis longtemps et les spécifications techniques sont prêtes. Deux banques sont déjà en pilote pour tester la plateforme de la Banque de France. Une fois la loi adoptée, nous pourrons alimenter l'outil dès septembre prochain.

Les banques et tous les prestataires de services de paiement seront tenus de l'alimenter. La Banque de France vérifiera par des contrôles sur pièces que chaque IBAN frauduleux identifié a bien été signalé. Nous avons insisté sur l'aspect immédiat : dès qu'un IBAN est identifié comme frauduleux, l'information doit être transmise le plus rapidement possible à la Banque de France. Le système est conçu pour fonctionner en temps réel, car sans cette réactivité, le dispositif perdrait toute utilité.

L'information sur les IBAN frauduleux sera transmise aux banques au moins une fois par jour, en temps quasi réel. Point important : une banque recevant un IBAN signalé comme frauduleux conserve sa capacité d'analyse. Si elle estime qu'il s'agit d'un compte légitime chez elle, comme celui d'un commerçant, elle peut corriger cette identification. L'outil permet d'éviter qu'un artisan ou une entreprise se retrouve

injustement bloqué par toutes les banques. Le signalement d'un IBAN ne provoque pas un blocage systématique, mais devient un élément d'information que chaque banque intègre dans son évaluation. Nous avons prévu cette capacité de correction immédiate pour éviter les désagréments. Ce point était crucial pour convaincre l'écosystème bancaire d'alimenter ce fichier, la Banque de France et la CNIL.

Daniel LABARONNE

L'outil sera effectif après la promulgation de la loi. Juridiquement, ma proposition de loi précise que le signalement doit se faire « sans délai », reprenant l'obligation déjà existante pour le signalement des mouvements suspects à Tracfin. L'idée est que le coût de signalement soit minimal pour les banques afin d'encourager la démarche. Un coût élevé dissuaderait les établissements de partager l'information. Nous visons un dispositif vertueux avec un coût le plus faible possible.

De la salle

Le groupe Crédit Agricole est ravi de cette initiative de partage des IBAN frauduleux qu'il soutient activement. Comme vous l'avez précisé, le partage d'information n'entraîne pas un blocage automatique mais enrichit notre *scoring.* Un IBAN signalé augmente légèrement le niveau de risque sans nécessairement tout bloquer. Par ailleurs, l'IBAN n'est qu'une première étape qui a prouvé son efficacité. Il faudra aller plus loin avec d'autres données. Comment y parvenir dans le respect du RGPD tout en servant l'intérêt légitime de nos clients ? Comment s'assurer que tous les établissements jouent réellement le jeu ?

Jean-François FILLIATRE

Je perçois une incitation à une nouvelle proposition de loi pour intégrer d'autres éléments face à l'évolution des fraudes.

Jérôme RAGUÉNÈS

Nous avons déjà mis en place des groupes de travail interbancaires sur la gestion de la fraude. Il n'y a pas de concurrence sur ce sujet visant à renforcer la résilience de l'écosystème. Franchissons d'abord cette première étape dans les prochaines semaines ou mois, et démontrons que l'outil fonctionne. Cette preuve nous permettra ensuite d'expliquer plus facilement aux législateurs et aux autorités que la fraude évolue et que nous devons enrichir cette base.

La loi prévoit que toutes les banques et tous les PSP participent. Si une banque constate des problèmes récurrents avec les IBAN d'un établissement particulier, les autorités de contrôle pourront vérifier que chaque institution alimente correctement le fichier.

De la salle

Merci pour votre soutien, Monsieur le Député. Les banques font déjà beaucoup contre la fraude et cet instrument va nous aider. Peut-être faudrait-il aussi examiner l'origine de la fraude. Par exemple, quand une opération frauduleuse sans double authentification est remboursée systématiquement par la banque, ne devrait-on pas responsabiliser les fournisseurs de messagerie qui facilitent la substitution d'IBAN

dans les e-mails ? Ne devraient-ils pas être tenus d'indemniser ces fraudes ? Comment la représentation nationale pourrait-elle s'intéresser à cette problématique ?

Jérôme RAGUÉNÈS

La question est encore plus large et concerne toutes les vulnérabilités de l'espace numérique. Nous avons pratiquement résolu la sécurisation des numéros de téléphone grâce à la loi Naegelen. Mais nous rencontrons encore beaucoup de difficultés avec les plateformes et les réseaux sociaux qui diffusent de fausses publicités et des sites frauduleux, générant des transactions contestées et remboursées par les banques.

Daniel LABARONNE

Je mesure l'ampleur du travail nécessaire pour répondre à votre demande. Je vous propose d'y réfléchir ensemble. Pour cette PPL, nous avons mobilisé beaucoup d'experts car nous ne prétendons pas tout savoir. Je suis ouvert à ce travail mais il faut se réunir. Actuellement, nous travaillons sur d'autres sujets, notamment la création d'un ordre des diagnostiqueurs de performance énergétique face aux fraudes liées au DPE. Préparez des propositions, et nous pourrons nous revoir en janvier prochain, si nous sommes encore en fonction. Vous avez raison, c'est un sujet dont le législateur doit s'emparer. Nous avons commencé à réfléchir pour les réseaux sociaux sur la protection des mineurs, mais il faudrait étendre cette réflexion au domaine économique.

Keynote : Fraude, l’évolution de la jurisprudence

Pierre STORRER

Je vais aborder la fraude au paiement, au sens des directives sur les services de paiement, sous l'angle juridique. Cette fraude est définie par l'Autorité bancaire européenne comme couvrant deux catégories : les opérations non autorisées et les opérations autorisées de manière frauduleuse. L'authentification forte du payeur, mesure phare de la DSP2, a bien fonctionné, poussant les fraudeurs vers la manipulation des payeurs, tendance que la DSP3 devrait mieux encadrer.

Pour lutter contre cette fraude, il y a trois approches. D'abord l'approche technologique, avec un paradoxe entre exigence d'instantanéité des paiements et nécessité de sécurité. Ensuite les comportements, non seulement des payeurs mais aussi des bénéficiaires, notamment les e-commerçants qui privilégient parfois la fluidité des paiements au détriment de la sécurité en utilisant de manière outrancière les dérogations à l’authentification forte qui ne figurent pas dans la DSP2 mais dans un règlement délégué.

Enfin, sur le plan jurisprudentiel, je note une évolution spectaculaire. Il y a quelques années, presque aucune jurisprudence n'existait sur les moyens de paiement au sens DSP1 et DSP2. Depuis le début de l’année, nous avons déjà plus d'une dizaine d'arrêts de la Cour de cassation sur la fraude au paiement - c'est considérable. La Cour de justice de l'Union européenne a posé les jalons avec trois arrêts fondamentaux, notamment l'arrêt CRCAM de 2021, qui établit que la responsabilité des prestataires de services de paiement pour des opérations non autorisées est exclusive.

On ne peut pas contourner le spécial par du général, le légal par du contractuel. C'est un arrêt fondamental qui a ouvert la voie. Un deuxième arrêt en 2023, encore plus important, l'arrêt Beobank, où la Cour reprend l'arrêt CRCAM et ajoute un élément fondamental qui servira de guide à la jurisprudence. Je vous lis le point 39 de cet arrêt : « Une juridiction nationale ne saurait ignorer la distinction consacrée dans la directive (DSP1) concernant les opérations de paiement selon qu'elles sont ou non autorisées et, partant, ne saurait se prononcer sur une demande de remboursement sans qualifier au préalable ces paiements d'opérations autorisées ou non. »

Tous les arrêts qui oublieront ce préalable seront censurés. Face à une demande de remboursement, il faut d'abord déterminer si l'opération a été autorisée ou non, car deux régimes différents s'appliquent.

Je salue également le travail des médiateurs bancaires qui, par leur action, contribuent à épuiser ce contentieux de masse lié à la fraude aux paiements qui représentent 80 % des saisines.

L'Observatoire de la sécurité des moyens de paiement a publié en 2023 treize recommandations relatives aux modalités de remboursements des opérations non autorisées, avec un arbre de décisions remarquable.

Qu'est-ce qu'une opération autorisée ? C'est une opération dont le payeur a consenti à son exécution. Le consentement vaut autorisation. La jurisprudence a précisé ce concept : consentir à une opération, c'est aussi consentir à son montant (arrêt de la Cour de cassation en 2021) et à son bénéficiaire (arrêt du 1er juin 2023). Si un paiement est réorienté vers un autre bénéficiaire par fraude, ce n'est pas une opération autorisée.

Pour le régime de responsabilité : une opération autorisée n'entraîne pas de remboursement, mais le droit commun de la responsabilité contractuelle (convention de compte) s'applique, par exemple le devoir de vigilance du banquier. Pour une opération non autorisée, c'est la responsabilité spéciale DSP1, DSP2 et bientôt DSP3 qui s'applique.

Enfin, l'arrêt dit *spoofing* du 23 octobre dernier précise que cette manipulation téléphonique ne caractérisait pas une négligence grave, et bien que le paiement ait été autorisé mais de manière frauduleuse, c'est le régime des opérations non autorisées qui s'applique.

Table ronde

Jean-François FILLIATRE

Sur la lutte contre la fraude, quelles actions sont menées au sein du GIE Cartes bancaires ?

Samuel WILLY, Responsable Data & Lutte contre la Fraude, Cartes Bancaires

La lutte contre la fraude fait partie de nos missions statutaires. C'est crucial car un outil de paiement sûr permet la confiance, sans laquelle il n'y a pas d'usage. Si vous avez une chance sur deux d'être fraudé, vous n'utiliserez plus votre carte.

Nous avons développé une vision à 360 degrés : nous travaillons avec les commerçants victimes de fraude, avec les forces de l'ordre pour assister leurs enquêtes, et avec l'écosystème bancaire (banques, Fédération Bancaire Française, Observatoire de la sécurité des moyens de paiement, Banque de France). Notre outil le plus efficace reste la détection de fraude en temps réel. Pour chaque transaction par carte CB, une analyse de risque en temps réel est effectuée. Notre objectif est de détecter les transactions frauduleuses pendant qu'elles se produisent, avant même que le propriétaire légitime ne s'en aperçoive. Nous envoyons une note de risque exploitée par la banque réceptrice. En partenariat avec Feedzai depuis plus d'un an, nous avons déployé des modèles d'IA en temps réel qui analysent plus de 200 points de données lors de chaque paiement en ligne pour détecter et empêcher la fraude.

Michèle HALLAK

Qu'observez-vous aujourd'hui comme tendances de fraude et qu'est-ce qui vous inquiète particulièrement ?

Samuel WILLY

Actuellement, la situation est plutôt bonne. Grâce à la DSP2, la fraude à la carte a significativement diminué, avec une réduction de plus de 40 % en vente à distance chez CB en cinq ans. Le système fonctionne bien, particulièrement l'authentification forte. Le maillon faible est désormais le propriétaire légitime du moyen de paiement. Les fraudeurs se sont professionnalisés et utilisent l'ingénierie sociale et la manipulation. Nous parvenons à détecter ces fraudes grâce aux outils de *scoring*, protégeant ainsi l'utilisateur contre lui-même.

Chez CB, nous allons plus loin avec la reconnaissance des appareils. En identifiant qu'un paiement provient de votre appareil habituel, nous ajoutons de la sécurité. Cela nous permet d'offrir du *frictionless payment* pour environ 50 % des transactions, avec un taux de fraude plus faible que pour les paiements avec authentification forte. Notre réseau français souverain, où les données restent en France, est trois fois moins fraudé que les autres réseaux de paiement.

Michèle HALLAK

Julien, qu'observez-vous comme tendances de fraude et qu'est-ce qui vous inquiète particulièrement ?

Julien GOULIAN, responsable du Département de Prévention et de Lutte Contre la Fraude, BNP Paribas Banque Commerciale En France

Pour les virements, qui contiennent très peu de données contrairement aux cartes, la tendance forte est l'ingénierie sociale où le client initie lui-même le virement. C'est extrêmement difficile à détecter car il n'y a pas d'intrusion dans la banque en ligne - tout est fait par le client. Le fraudeur crée un véritable tunnel mental où le client perd conscience de ses actes. L'interaction fraudeur-client peut durer plusieurs heures, jours ou semaines, tandis que notre traitement d'alerte est beaucoup plus court. Le client nous cache souvent le vrai motif ou ment sur ses intentions. Nous devons professionnaliser nos interactions et développer des outils pour faire sortir le client de ce tunnel, l'alerter sur le caractère inhabituel de l'opération, au-delà de la simple logique.

Jean-François FILLIATRE

Existe-t-il une typologie des victimes de fraude ?

Julien GOULIAN

Les jeunes sont les personnes les plus vulnérables, contrairement à ce qu'on pourrait croire, avec une grande naïveté sur les réseaux sociaux.

Michèle HALLAK

C'est surprenant. J'ai récemment entendu une étudiante raconter comment elle s'était fait arnaquer de 5 000 euros en quelques minutes. Luis, du point de vue d'un fournisseur technologique, quelles tendances observez-vous en France, en Europe et au-delà ?

Luis JUNES, expert en prévention de la fraude, Feedzai

Nous observons depuis plus de cinq ans la montée des fraudes autorisées, c'est-à-dire des arnaques. Ce phénomène va s'amplifier avec le développement du paiement instantané en Europe, non seulement via virements IBAN mais aussi avec les nouveaux moyens de paiement de compte à compte comme Wero ou Bison.

La temporalité est une variable cruciale pour lutter contre cette fraude. Les attaques peuvent s'étendre sur plusieurs mois, comme le « pig-butchering » où les fraudeurs ciblent une victime et obtiennent progressivement son argent sur une longue période. La clé est d'analyser une période assez large en temps réel, au moment de la transaction. Par exemple, détecter qu'un bénéficiaire a été ajouté deux minutes avant ou qu'un IBAN a reçu de nombreux virements récemment. D'autres signaux comme une session bancaire anormalement longue ou un appel en cours peuvent aussi alerter. L'analyse du comportement passé est essentielle pour comprendre la nature de la transaction en temps réel.

Jean-François FILLIATRE

Julien, Pierre Storrer a dit qu'on ne peut pas avoir à la fois l'instantanéité et la sécurité. Quelle est votre position ?

Julien GOULIAN

C'est toujours un équilibre entre expérience client et protection. Dans la lutte contre la fraude, le moyen idéal serait qu'il n'y ait pas de moyens de paiement, mais ce n'est pas viable. Il faut trouver le juste équilibre entre sécurité et fluidité - entre simplement alerter le client et lui interdire certaines actions. C'est un ajustement permanent, d'autant plus important que le moyen de paiement est au cœur du métier bancaire, avec une responsabilité de non-immixtion.

Jean-François FILLIATRE

Samuel, vous mentionniez l'utilisation de l'IA. Quel pourcentage de fraudes détecte-t-elle ? Et parmi les opérations signalées comme frauduleuses, combien le sont réellement ?

Samuel WILLY

Nos exigences sont très élevées et définies avec les banques. Nous ne refusons jamais de transaction nous-mêmes, c'est toujours la banque qui prend cette décision avec son client. Notre objectif est qu'au moins une transaction sur deux que nous préconisons de refuser soit effectivement frauduleuse. Pour les paiements en ligne utilisant 3DS, nos taux de fraude sont inférieurs à 0,06 % (six fraudes sur 10 000 paiements). Grâce à notre analyse de risque, nous détectons une fraude sur deux, en écartant la majorité des paiements légitimes pour cibler très précisément la fraude. Concernant l'IA, nous estimons qu'elle représente environ 50 % de ce que nous détectons. Cependant, la connaissance métier et l'expertise humaine restent tout aussi importantes. Nos modèles d'IA sont d'ailleurs enrichis par les échanges entre nos *datascientists* et nos experts fraude.

Jean-François FILLIATRE

Quel modèle d'IA utilisons-nous concrètement ? Il existe de l'IA générative et de l'IA historique. Pour l'IA générative, se pose notamment la question des hallucinations. L'IA utilisée pour la fraude est-elle susceptible de générer des hallucinations ou s'agit-il d'un autre type d'IA ?

Samuel WILLY

Chez CB, nous n'utilisons pas d'IA générative. Les algorithmes génératifs sont extrêmement complexes, longs à exécuter et coûteux. Or, nous devons scorer 12 milliards de transactions par an en temps réel, ce qui impose des exigences très strictes en termes de temps de calcul. Nous travaillons avec des données que nous maîtrisons parfaitement et obtenons d'excellentes performances avec des modèles d'IA existant depuis quelques années mais à la pointe dans la détection de fraude. L'IA générative n'est pas la plus adaptée à notre cas d'usage.

Jean-François FILLIATRE

Qu'en est-il chez BNP Paribas ?

Julien GOULIAN

De manière générale, ce que Willy vient d'expliquer relève du *machine learning*. L'IA générative n'est pas du tout à l'ordre du jour actuellement.

Luis JUNES

L'IA est un grand parapluie qui couvre plusieurs méthodologies. Plus précisément, nous utilisons des modèles de *machine learning* supervisés qui apprennent à partir de données historiques. C'est pourquoi les biais sont importants, comme dans l'anecdote sur le crédit refusé à une femme - le modèle avait appris des biais humains. Pour lutter

contre la fraude transactionnelle côté banque d'émission, ces modèles fonctionnent très bien, notamment l'AZBM et Exiboost. L'IA générative, quant à elle, sera plutôt utilisée par les opérationnels pour accélérer l'analyse et l'investigation une fois qu'une alerte a été générée par le système.

Michèle HALLAK

J'ajouterais l'automatisation des rapports SAR et quelques solutions pour aider les clients finaux à détecter les escroqueries, bien que l'IA soit surtout utilisée par les fraudeurs. Samuel, avez-vous constaté une explosion des fraudes liées à l'IA ?

Samuel WILLY

Les forces de l'ordre sont mieux placées pour en parler car elles remontent les filières. D'après nos échanges, l'IA générative aide effectivement les fraudeurs. Il y a cinq ans, on recevait des mails d'arnaque remplis de fautes d'orthographe facilement identifiables. Aujourd'hui, c'est plus sophistiqué, et l'IA a fait tomber la barrière de la langue pour les fraudeurs. Auparavant, ils ciblaient surtout les pays correspondant à leur langue maternelle. Le Monde a récemment révélé l'existence de logiciels chinois commercialisés par des pirates, capables de générer des milliers d'e-mails dans n'importe quelle langue pour du phishing. La fraude se professionnalise avec l'IA générative qui facilite la création de contenus servant à l'hameçonnage.

Julien GOULIAN

Une autre tendance concerne les escroqueries comme la fraude au sentiment. L'IA générative permet de diffuser sur les réseaux sociaux du contenu complètement faux, comme ces fausses annonces supposément sponsorisées par Élise Lucet. Un cas m'a été signalé où un soi-disant livret offrait 400 € d'intérêts quotidiens pour un dépôt de 4 000 €, réservé aux clients VIP. Un prospect s'est présenté en agence BNP pour supplier d'avoir accès à ce produit inexistant.

Michèle HALLAK

Luis, pouvez-vous nous parler du profil du fraudeur ?

Luis JUNES

C'est un sujet intéressant car il existe toute une industrie de la fraude avec ses propres victimes. Des bandes criminelles organisées, notamment d'Asie, exploitent des immigrés dont les passeports sont confisqués et qui sont enfermés pendant des mois à escroquer l'Occident. Ils sont spécialisés dans la fraude autorisée (escroqueries) et l'IA générative va considérablement accroître leur efficacité. Lutter contre ce type de fraude, c'est aussi protéger ces victimes et combattre une industrie proche de l'esclavage.

Julien GOULIAN

En France, je n'ai pas connaissance de ce type de cas. Il s'agit plutôt du jeune arnaqueur depuis son canapé.

Luis JUNES

J'ai une vision globale car nos clients sont principalement aux États-Unis et au Royaume-Uni. En France, il est intéressant de noter que ces arnaqueurs individuels

sont faciles à détecter grâce à la biométrie comportementale. Quand la fraude est industrialisée, nous détectons d'autres types de signaux, comme des *bots*, qui ne correspondent pas à des comportements humains.

Michèle HALLAK

On observe ces réseaux d'escroqueries avec des victimes enrôlées, particulièrement en Asie. Samuel, concernant les solutions que vous avez mises en place, quels sont les freins à l'adoption de l'IA ?

Samuel WILLY

Nous utilisons depuis longtemps l'IA ou le *machine learning* pour analyser l'ensemble de nos données, repérer les commerçants attaqués et établir des profils de carte afin d'identifier les activités suspectes. Nous sommes passés à l'IA en temps réel depuis environ un an, et le système basé sur les *devices* entrera en production le mois prochain après la phase pilote actuelle.

Concernant les freins, développer des modèles de *machine learning* est complexe et chronophage. Il faut d'abord identifier des cas d'usage pertinents. Ensuite, dans la lutte contre la fraude, nous devons constamment trouver l'équilibre entre le RGPD et la LCLF, en établissant un cadre réglementaire permettant d'exploiter au mieux les données tout en respectant la protection des données personnelles.

Michèle HALLAK

Julien, quelles sont selon vous les meilleures pratiques en matière d'IA et les freins rencontrés ?

Julien GOULIAN

Le frein principal est le respect de la loi. Le RGPD impose de demander le consentement au fraudeur pour le surveiller, ce qui est délicat. Les mécanismes de surveillance comportementale et de *call in app* sont soumis à l'examen de la CNIL. Je rappelle que le motif d'utilisation de lutte contre la fraude n'est pas encore pleinement acté dans le RGPD. Les limites de ce qu'on peut faire en matière de biométrie comportementale restent floues.

Michèle HALLAK

Comment voyez-vous ce paysage évoluer dans les années à venir pour se projeter ? Qui prend la question pour commencer ?

Jean-François FILLIATRE

Je vais compléter la question. La fraude est un jeu du chat et de la souris. D'un point de vue technologique, quel est notre retard sur les fraudeurs ? Se compte-t-il en mois ou en semaines ?

Julien GOULIAN

Ce ne sont pas des retards technologiques. La fraude est comme l'eau qui coule - on met la main, mais ça continue. C'est trop d'argent facile et moins risqué que d'autres activités illégales. C'est une course sans fin. Notre défi est de mettre des sécurités,

mais le fraudeur va s'adapter à ces barrières. Ce n'est pas une question technologique mais plutôt la capacité du fraudeur à manipuler et contourner nos protections.

Jean-François FILLIATRE

À partir de quel moment une nouvelle typologie de fraude devient-elle visible ? Est-ce massif et rapidement détecté, ou monte-t-elle à bas bruit, permettant son développement avant que les établissements puissent la détecter et y répondre ?

Julien GOULIAN

Il existe des phénomènes de fond. Le *phishing* est en chute libre, remplacé par les *scams* et l'ingénierie sociale. Parallèlement, des typologies ponctuelles apparaissent, comme la fraude WhatsApp où quelqu'un usurpe un compte pour demander de l'argent à des contacts. Il n'y a pas vraiment de règle.

Samuel WILLY

Nous surveillons la fraude quotidiennement. Toute nouvelle typologie générant des montants significatifs est rapidement détectée. Notre approche est pragmatique : viser là où l'eau passe le plus. Dans ce jeu du chat et de la souris, nous observons une tendance de fond à la baisse. Pour l'avenir, le désir croissant de fluidité et d'instantanéité des paiements s'accompagne d'exigences de sécurité accrues. La solution passe par l'analyse de données en temps réel, décloisonnant des environnements de paiement encore trop souvent silotés, et exploitant des outils sophistiqués pour offrir fluidité et détection précise.

Luis JUNES

Les systèmes actuels détectent les nouvelles tendances de fraude. Le problème survient quand ces attaques deviennent fréquentes et impactent nos systèmes. L'*account take-over* diminue car nous avons déployé des solutions comme la biométrie comportementale et les notifications de protection. Pour la fraude autorisée, nous constatons que l'analyse en temps réel sur de larges fenêtres temporelles (12 mois ou plus) est essentielle, combinée aux données contextuelles et à l'historique client. Nous continuons à explorer les meilleures approches pour l'avenir.