Comment l'utilisation de la donnée a-t-elle permis une évolution dans la lutte contre la fraude monétique ?

Walid Becherif

le cnam

Mémoire

pour l'obtention du

Master Sciences humaines et sociales

mention humanités numériques

Parcours Mégadonnées et analyse sociale (MEDAS)

Comment l'utilisation de la donnée a-t-elle permis une évolution dans la lutte contre la fraude monétique ?

Walid BECHERIF

Date et lieu de la soutenance

- 09 septembre 2021
- CFA CNAM SAINT-DENIS (93)

Membres du jury

- Ghislaine Chartron, Présidente du Jury
- Josselin Noirel, Tuteur Pédagogique

Promotion (2020-2021)

Ce mémoire a pour sujet la fraude à la carte bancaire. Axé sur la compréhension du système monétique, il s'attachera à comprendre les différents mécanismes de la fraude à la carte bancaire, ainsi que les impacts que la fraude peut avoir en volume et en coût.
Nous essayerons de comprendre comment la donnée peut-elle apporter une réponse aux problématiques liées à la fraude monétique.

Descripteurs

Banque
Fraude à la carte bancaire
Système monétique
Interopérabilité
Données Massive
Science de la donnée
Apprentissage Automatique
Modèle de données
Europe
Sepa

This dissertation is about bankcard fraud, focused on the understanding of the electronic banking system, it will focus on understanding the different mechanisms of bankcard fraud, as well as the impacts that fraud can have in volume and cost.
We will try to understand how the data can bring an answer to the problems related to the electronic banking fraud.

Keywords

Bank
Credit Card Fraud
Monetic System
Interoperability
Big-Data
Data-science
Machine Learning
Data model
Europe
SEPA

Remerciements

Avant toute chose je tenais à remercier les collaborateurs BforBank ainsi que l'équipe pédagogique notamment :

Josselin NOIREL, pour sa disponibilité et son implication au cours de cette année d'alternance.

Florian DELPUCH, pour m'avoir donné la possibilité de travailler dans cette équipe et m'avoir suivi tout au long de ma première année.

Florian DUCHAT, pour son implication dans ce mémoire et tout le suivi à la suite de la passation.

Faustine GUSTO, Nassim SIDHOUMI et Marion ANDLAUER pour leurs conseils et leurs disponibilités.

Introduction

Le monde bancaire est très ancien, les banques se sont toujours adaptées aux évolutions de la société. Avec l'émergence de nouvelles technologies et une digitalisation accrue, il paraissait normal qu'elles suivent cette tendance. C'est ainsi qu'au cours des deux dernières décennies, les banques se sont beaucoup digitalisées, et, in fine certaines 100% digitales ont commencé à apparaître.

Les besoins des clients ont évolué, ils cherchent à être plus autonomes, à avoir l'information rapidement et simplement.

Le marché des banques en ligne est un marché récent, mais très concurrentiel avec beaucoup de grands acteurs qui se partagent ce marché.

Le groupe Crédit Agricole a, en 2009, lancé sa banque 100 % digitale, BforBank. Au départ, BforBank était une banque d'épargne avec pour seul produit des livrets, de l'assurance-vie et de la bourse.
En 2015, il a été décidé de lancer un service de banque au quotidien afin d'augmenter le capital client.
Toujours sur cette stratégie en avril 2017, le crédit immobilier a été lancé.

Comme dit précédemment le marché des banques en ligne est très concurrentiel et pour se démarquer, il faut pourvoir proposer des offres très intéressantes, avec une tarification avantageuse pour le client. Il faut aussi très bien connaître le besoin du client afin de lui proposer des produits adaptés à son besoin comme de l'épargne, de l'assurance-vie ou de la bourse.

C'est à cet effet que les banques en ligne investissent dans des domaines innovants comme l'intelligence artificielle et la data-science. D'une part, les données clients permettent de mieux comprendre leurs besoins et l'intelligence artificielle permet l'automatisation de certaines tâches pénibles, ce qui permet en plus de gagner du temps d'économiser certains coûts et donc de réduire la perte due aux primes de bienvenue, par exemple, ou encore de limiter les coûts liés à la fraude monétique ou la fraude identitaire.

La fraude à la carte bancaire, aussi appelée fraude monétique est un véritable enjeu pour les banques, notamment pour les banques en ligne qui cherchent à améliorer leur rentabilité et dégager un bénéfice net.
Plusieurs centaines de millions de cartes de paiements étaient en circulation en 2020. Face à l'augmentation de l'utilisation de ce moyen de paiements pour en faire aujourd'hui le moyen de paiement préféré des Français, cet engouement en fait aussi, le moyen de paiement le plus fraudé aujourd'hui en France et en Europe.
La cybercriminalité est aujourd'hui omniprésente dans ce secteur et les fraudeurs utilisent de nouveaux moyens toujours plus ingénieux.
Le corollaire de cette grande popularité est que nous possédons un grand nombre de données concernant les transactions bancaires, et parmi celles-ci, les transactions frauduleuses. Dans un monde où l'utilisation de la donnée est devenue un atout pour les entreprises, nous

essayerons de comprendre comment l'utilisation de la donnée a-t-elle permis une évolution dans la lutte contre la fraude monétique ?

Pour ce faire nous présenterons dans un premier temps le système monétique dans son ensemble, puis nous nous attacherons à présenter la fraude à la carte bancaire notamment le type de fraude, les montants engagés et les moyens de lutter contre celle-ci.
Enfin nous effectuerons une étude de cas dans un contexte de banque en ligne afin d'observer si l'utilisation de la donnée permet de détecter et de réduire la fraude.

1) Présentation de l'entreprise

BforBank est principalement financée par les caisses régionales du Crédit Agricole et Crédit Agricole S.A, elle propose une tarification avantageuse tout en conservant une image haut de gamme. En effet, jusqu'à récemment le revenu minimum pour pouvoir ouvrir un compte chez BforBank était de 1600 € Net par mois.
Depuis octobre 2018, une offre de carte classique a été lancée avec un seuil minimal de revenu de 1200 € Net par mois.

BforBank étant une banque 100% en ligne, elle ne dispose pas d'agences physiques ; celles-ci sont remplacées par un Service Relation Client, joignable du lundi au vendredi de 8h à 21h et le samedi de 9h à 18h par téléphone, email, chat et réseaux sociaux.

Les services BforBank sont accessibles depuis le site web ou l'application mobile. Une très grande partie des opérations est réalisable depuis le site ou l'application mobile.

Étant le premier lien entre le client et BforBank, le site et l'application mobile ont été pensés pour être simples et rapides, afin de permettre aux clients d'effectuer leurs opérations en toute simplicité.
BforBank compte aujourd'hui 260 000 clients.

1.1) Structure de l'entreprise

BforBank compte environs 290 salariés répartis dans 6 Directions :

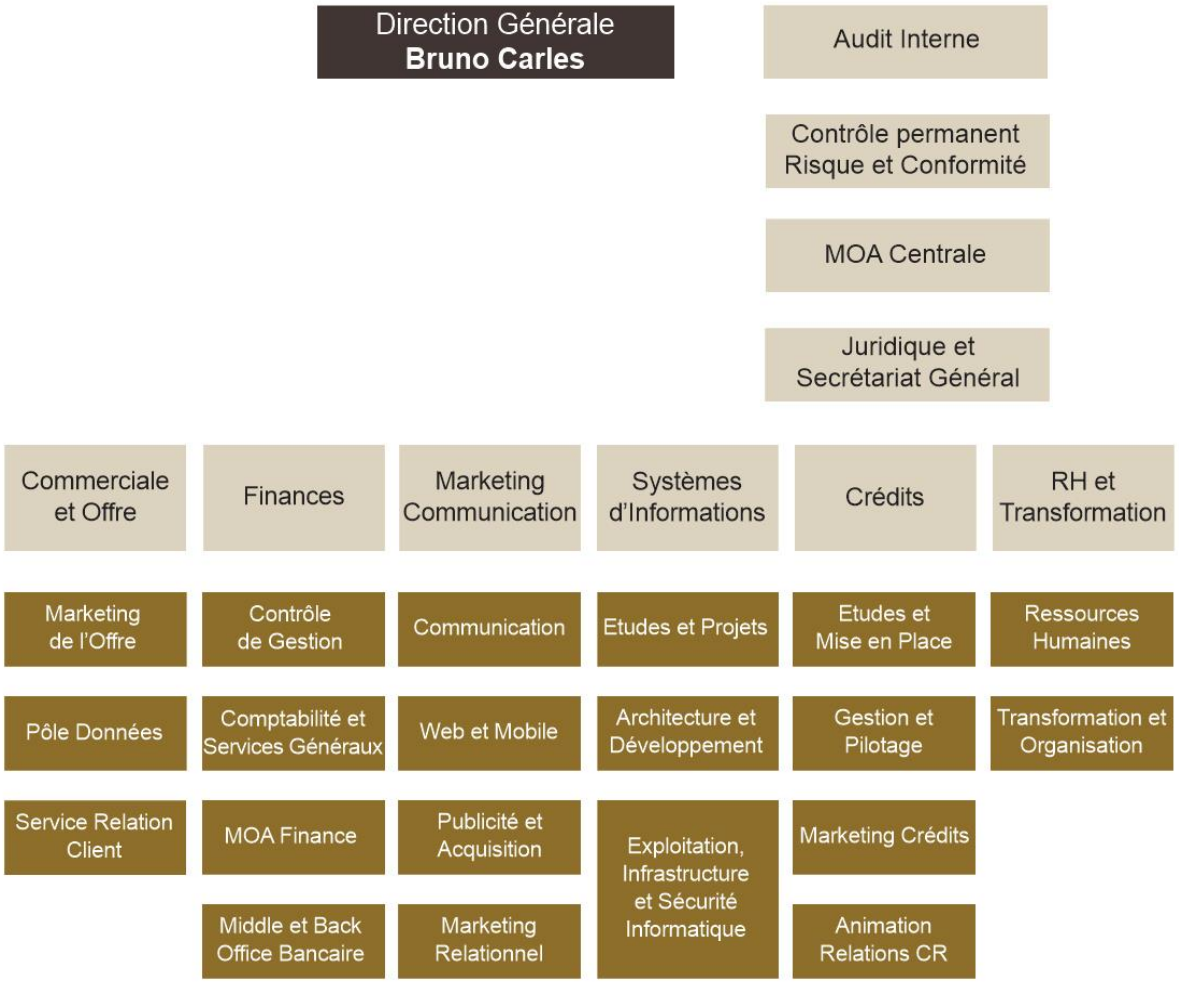


Figure 1 : Organigramme BforBank (Source : Interne)

1.1.1) Les produits proposés par BforBank

- L'Assurance-Vie (AV)

Il s'agit d'un produit d'épargne à moyen/long terme qui permet de valoriser et diversifier son capital. Il est également le produit d'épargne préféré des Français. C'est un contrat diversifié avec plusieurs placements possibles, en effet il est possible de choisir soi-même ses supports financiers, d'être accompagné dans le choix des placements ou de déléguer la gestion de son investissement à des professionnels.

- La Bourse

Le produit Bourse permet à des investisseurs novices ou avertis de placer leur argent en Bourse. BforBank donne accès gratuitement à des outils performants d'aide à la décision.

- Le Livret A et le Livret Développement Durable (LDD)

Produits d'épargnes avec un taux réglementé. Contrairement au Livret d'épargne BforBank, les intérêts sont exonérés des prélèvements sociaux et des impôts sur le revenu. Pour pouvoir

souscrire à ces produits, BforBank doit être la banque principale du client (il n'est pas possible d'avoir plusieurs Livrets A ou LDD).

- Le livret d'épargne BforBank (CSL)

Historiquement il s'agissait du produit phare de BforBank. Un livret au placement garanti, doté d'un plafond de 4 millions d'euros.

Le calcul des intérêts est effectué par quinzaine ce qui veut dire que :

- Les fonds déposés du 1er au 15 du mois commencent à produire des intérêts à partir du 16
- Les fonds déposés du 16 au dernier jour du mois produisent des intérêts au 1er du mois suivant.

Les intérêts sur les fonds cessent de courir à la fin de la quinzaine qui précède le jour du retrait.

Au départ, le livret disposait de taux extrêmement avantageux, qui se sont dégradés avec les années.

- Les crédits à la consommation

L'offre de crédit est réservée uniquement aux clients BforBank. Trois types de prêts existent, le prêt personnel (d'un montant compris entre 1 000€ et 75 000€), le prêt Auto (d'un montant compris entre 3 500€ et 100 000€) et le prêt Travaux (d'un montant compris entre 3 500€ et 46 000€).

- Le compte bancaire

BforBank propose une Carte Visa Premier gratuite pour toutes personnes majeures disposant d'un salaire net mensuel d'au moins 1 600€.

Historiquement, BforBank ne proposait que les produits cités ci-dessus. Dans un souci d'accroitre sa clientèle ainsi que son positionnement, le compte bancaire est lancé en 2015.

Il est important de le noter, car les clients dits « historiques » et les « nouveaux clients » n'ont pas le même comportement.

- Le crédit immobilier

BforBank a lancé en avril 2017 une offre de Crédit immobilier. Le crédit immobilier BforBank dispose de nombreux atouts :

- Des taux compétitifs, parmi les meilleurs du marché et sans contrepartie
- La liberté d'ouvrir un compte ou non chez BforBank
- Frais de dossiers offerts
- Pas d'indemnité de remboursement anticipé
- Un parcours simple et rapide
- Un Espace de Suivi sécurisé pour être informé en temps réel de l'avancement du dossier et gérer toutes les étapes de la demande de financement

1.1.2) Présentation du Pôle Data-Science & Analytics

Le Pôle Data-Science & Analytics analyse les données clients à travers divers aspects (comportements clients, données de navigation, résultats des actions marketings, parcours de souscription, etc.). Ces informations sont ensuite fournies aux différents services de la banque et permettent ainsi une précieuse aide à la décision.

L'équipe est composée :

- D'un responsable
- De deux Data-Analyst.
- D'un Data-Scientist*.
- D'un alternant.

Schéma de données BforBank

Les données BFORBANK sont entreposées dans un Data-Warehouse (DWH) , les données de la veille sont ajoutées chaque nuit via un batch.
Les données proviennent de différentes sources, une grande partie de nos données proviennent de T24 un progiciel bancaire.

Les données de navigation nous sont fournies à l'aide du service XITI d'AT Internet, les données d'assurance-vie et de bourse nous sont fournies respectivement par Spirica et CA Titres. Enfin, les données concernant le contact client nous sont remontées via notre outil CRM.

Les données propres au SRC (nombre d'appels reçus/traités, durées des appels, etc.) ne sont pas remontées dans le Data-Warehouse. Ces données sont accessibles via les interfaces de nos partenaires (Odigo pour les appels, Eptica pour les e-mails et enfin Dimelo pour les réseaux sociaux).

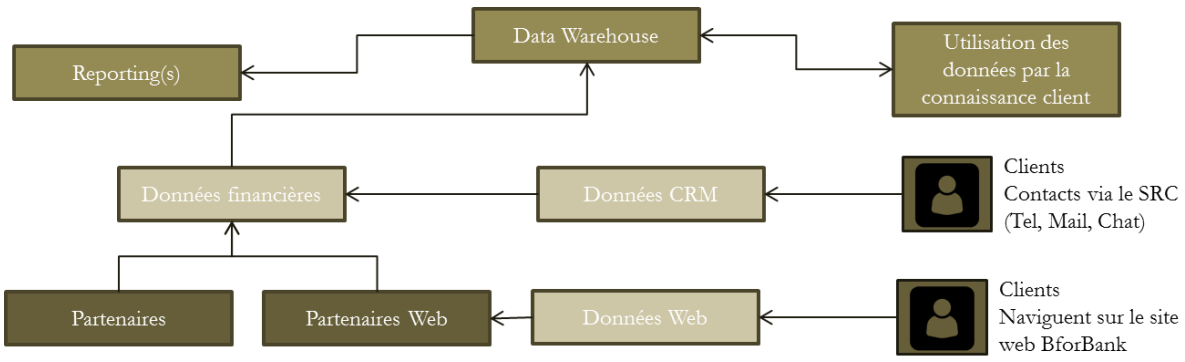


Figure 2: Schéma de données BforBank (Source : Interne)

1.1.3) Présentation de mes missions

La mission principale de mon alternance était la mise en place de nouveaux reportings suivant le besoin des différentes équipes qui composent BforBank. Au cours de mes deux années d'alternance, j'ai pu ainsi travailler avec toute la donnée BforBank, apprendre à découvrir sa profondeur et sa complexité. J'étais aussi en charge de la mise à jour et du maintien du process d'automatisation de nos reportings.

Le métier de Data Analyst comprend également de nombreuses autres missions qui me seront confiées lors de mon alternance. Le maintien ou la refonte de score, la gestion de projet au travers d'un projet de migration de serveurs et plusieurs études ponctuelles en font partie.

1.1.4) Traitement de la fraude monétique chez BforBank

La fraude monétique est traitée par le MO Flux & Paiements chez BforBank, une équipe composée de plusieurs collaborateurs. Ceux-ci vont analyser les déclarations d'utilisation frauduleuse des clients (vérification des caractéristiques de la transaction, utilisation de la double authentification, montant de la fraude, etc.) et décident de procéder à un remboursement ou non-remboursement.

Si le remboursement est accepté, la banque contacte son prestataire gérant la carte bancaire afin que celui-ci procède au recouvrement de la somme auprès du commerçant.

Une fois l'analyse effectuée, ils vont référencer le dossier dans un fichier Excel unique, contenu lui-même dans un dossier. Une copie du dossier est aussi sauvegardée au format PDF.
Ce traitement manuel semble obsolète au vu des possibilités technologiques disponibles aujourd'hui. De plus, cela pose un problème dans le traitement de la fraude, car les transactions frauduleuses restent au service Flux & Paiement et ne remontent pas dans nos bases de données.

2) État de l'art

2.1) Contexte

La carte bancaire est en 2021 le moyen de paiement le plus utilisé dans les pays développés, tant pour des paiements de proximité que pour des achats sur Internet. En 2020, pour la première fois les Français ont plus utilisé la carte bancaire comme moyen de paiement que l'espèce. Cette utilisation massive de moyen de paiement électronique couplé à l'instantanéité de ces mêmes moyens de paiements entraîne des problèmes de sécurité importants.
On constate une augmentation de la fraude à la carte bancaire au fil des années, et ce malgré de nombreux nouveaux outils aidant à lutter contre celle-ci.

2.2) La monétique

La monétique est un système qui s'appuie sur plusieurs acteurs, qu'ils soient des particuliers, des acteurs bancaires ou étatiques.
La monétique fonctionne souvent sur un système appelé « 4 coins » ou encore système de tokenisation.

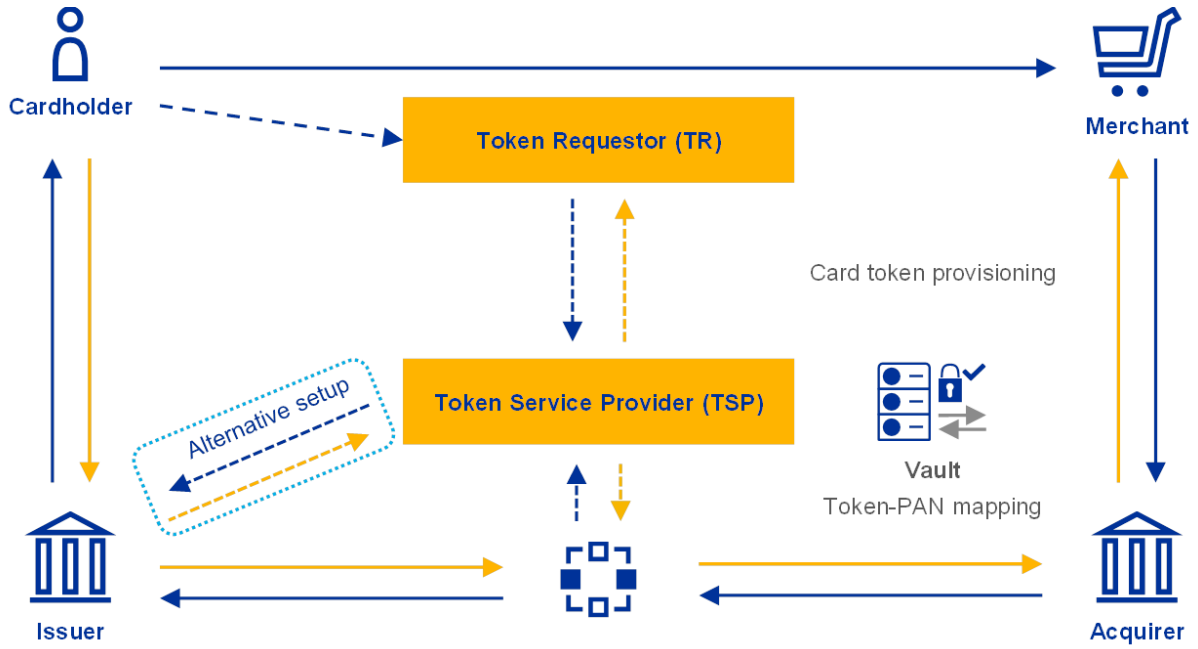


Figure 3 : Schéma du système monétique (Source : https://www.ecb.europa.eu)

Ainsi, lors d'un classique paiement par carte, le client (Cardholder) insère sa carte dans l'appareil du commerçant (Merchant). Il se peut que l'appareil contacte la banque du commerçant (Acquirer), qui, via le réseau de routage (Token Service Provier), va interroger la banque du client (Issuer) afin de savoir si le paiement peut être effectué.

2.2.1) Les systèmes de paiements

Pour qu'un paiement par carte puisse s'effectuer, il doit être identifié par un système de paiement : la carte affiliée au système de paiement en question sera donc reconnue et acceptée chez le marchand adhérant au même système de paiement.
Dans le cas de BforBank, la carte bancaire est affiliée pour la France au réseau Carte bleue (CB) et pour l'international au réseau Visa. Cette coexistence de 2 systèmes de paiement sur une carte bancaire permet de limiter les frais d'usages pour les paiements domestiques tout en offrant la possibilité d'effectuer des paiements à l'étranger via le réseau Visa.
Il existe aujourd'hui 2 principaux systèmes de paiement internationaux Visa et Mastercard.
Depuis 2013, les frais pour l'acquéreur ont sensiblement diminué, sous l'impulsion de l'autorité de la concurrence.
Il est à noter qu'actuellement un système de paiement interbancaire européen est en cours de création, regroupant 16 banques dans 5 pays européens. [1]

2.2.2) La place du terminal de paiement

Le rôle du terminal dans le système monétique est principalement de faire l'interface entre la carte et le réseau d'acquisition et de paramétrage.
Il n'en demeure pas moins un élément actif, en charge de :

- La réception des paramétrages acquéreurs ;
- La sélection des applications de paiement ;
- L'évaluation et acception/refus d'une transaction ;
- Véhiculer et opérer la transaction.

2.2.3) La sécurité du système monétique

La « Credit card association » [2], organisation américaine a engagé la responsabilité des banques des commerçants et des systèmes de paiements à appliquer des standards de sécurité. S'ils ne sont pas respectés, des sanctions sont applicables, dont :

- Des pénalités financières
- L'exclusion de l'adhésion aux systèmes de paiements
- Le retrait de terminal de paiement

Pour satisfaire ces exigences, 12 critères sont à minima à remplir :

1. Un pare-feu sécurisé protégeant les données des titulaires de carte
2. L'utilisation de mots de passe élaborés pour tout paramètre de sécurité
3. Protéger les données contenues dans la carte bancaire
4. Crypter les données lors des transactions
5. Utilisation d'outils de cyber sécurité performants, et les mettre à jour
6. Maintenir à jour les applications utilisées, notamment les patchs de sécurité
7. Restreindre l'accès aux données des titulaires de cartes aux personnes qui en ont un réel besoin
8. Utilisation d'un identifiant unique par utilisateur
9. Restreindre l'accès physique aux cartes bancaires
10. Pouvoir suivre qui accède aux données clients
11. Tester régulièrement les processus de sécurité
12. Avoir une politique de traitement de l'information sécurisé

Des audits peuvent avoir lieu pour valider ces critères.

2.3) La carte bancaire

2.3.1) Historique de la carte bancaire dans le monde moderne

Débutant sur un support en carton pour finir dans nos smartphones, la carte bancaire a aujourd'hui plus d'un demi-siècle.

En 1946, Jon Biggins [3] de la « Flatbush National Bank of Brookliyn » invente la « Charg-it card » afin de faciliter les crédits ; ainsi, quand un client utilisait sa carte, une facture était émise à sa banque. Cela permettait aux clients de ne pas payer immédiatement ; pour la première fois, la banque payait à la place du client en lui faisant crédit.

Figure 4 : Première carte de paiement à crédit (Source : Google Image)

Peu de temps après, en 1950, Diner's Club créa sa carte de crédit avec laquelle il était possible de payer ses repas et ses dépenses dans l'enseigne et ses enseignes partenaires. Elle est communément aujourd'hui connue comme étant la première carte de crédit ayant eu beaucoup plus de notoriété que la « Charg-it card ». Plus tard, la carte produite par Diner's Club se diffusera dans le monde entier.

Figure 5 : Carte du Diner's Club (Source : https://www.dinersclub.com/about-us/history)

La carte de paiement n'abandonne le support cartonné qu'en 1959 lors du lancement de la première carte plastique par American Express (figure 2.1b).

Cependant, ces cartes demeurent privatives et il faut attendre les années 1960 pour voir l'émergence de l'interbancarité avec la création de BankAmericard en 1958 (devenu Visa) et d'Interbank Card Association en 1966 (devenu MasterCard Worldwide).

2.3.2) EMV

L'Europay Mastercard Visa (EMV) créée en 1996 est aujourd'hui le standard de sécurité des cartes de paiements (carte à puce uniquement), il est géré par l'EMVCo.

Les spécifications de l'EMVCo se regroupent en 4 livres :

1. Interface entre le terminal de paiement et la carte de paiement
2. Sécurité
3. Applicatif
4. Interface entre le propriétaire de la carte, le marchand et l'acheteur

Une transaction avec l'EMV s'effectue comme-ci :

1. Sélection de l'application (système de paiement partenaire VISA, MASTERCARD, CB, etc.)
2. Initialisation de l'application
3. Lecture des données
4. Analyse des restrictions
5. Analyse et authentification des données hors-ligne
6. Authentification du porteur
7. Analyse du terminal
8. Action du terminal paiement accepté, refusé, etc.)

Depuis la démocratisation des paiements sans contact, et encore plus depuis la crise du covid, l'EMVCo a émis des spécifications spécialement pour les paiements utilisant la technologie du sans-contact avec 3 livres (V.2.10):

- Livre A : Architecture et exigence générale
- Livre B : Point d'entrée
- Livre C : Spécification technique

Toutes ces étapes permettent de sécuriser les transactions, notamment les transactions hors ligne, il permet de réduire la fraude par rapport aux transactions effectuées par carte magnétique.

2.3.3) La carte de paiement en France

L'apparition de la carte bancaire en France est plus tardive puisqu'elle date de 1967 et ne permet initialement que de réaliser des opérations de retrait dans les distributeurs automatiques de billets de son établissement bancaire ; l'interopérabilité entre les banques n'est pas encore développée.
Les cartes internationales, permettant des retraits et paiements en France et à l'étranger, apparaissent en 1973 avec l'arrivée de Visa.

Le Groupement des Cartes bancaires est créé en 1984 et permet l'interopérabilité bancaire. En 1986, les premières cartes à puces font leurs apparitions et permettent le paiement sécurisé par code.

En 1998, les banques françaises se soumettent à la norme internationale EMV (Europay-Mastercard-Visa), qui est un protocole de paiement et de retrait créé en 1996. [4]

Afin de présenter le fonctionnement des cartes de paiement et de pouvoir en étudier la fraude, il est nécessaire d'introduire la notion d'interfaces d'interaction des cartes de paiement ; une interface étant un des moyens pour le terminal ou le commerçant d'interagir et dialoguer avec la carte.
Chaque carte peut ainsi être dotée, à l'heure actuelle, d'un maximum de quatre interfaces :

- L'interface visuelle ;
- L'interface magnétique ;
- L'interface puce à contacts ;
- L'interface puce sans contact.[5]

Figure 6 : Exemple d'une carte de paiement (Source : Interne)

2.3.4) Les interfaces de la carte de paiements

Figure 7 : Interface visuelle d'une carte de paiements (Source : Interne)

a) Interface visuelle

L'interface visuelle comporte plusieurs informations :

1. Le numéro de la carte
2. Le nom du propriétaire de la carte
3. Date d'échéance
4. Système de paiement
5. Indication de la présence due sans contact
6. Type de carte (Débit différé ou immédiat)
7. Signature
8. Cryptogramme
9. Hologramme de sécurité

b) La carte à puce

La carte à puce est en général une carte en plastique dans laquelle est apposé un microcontrôleur, celui-ci permet l'échange de différentes informations, notamment dans le cadre du protocole EMV.

Malgré la migration très tôt des cartes à puce en France et en Europe, celle-ci reste peu développé aux États-Unis [6]

	2017		2018		2019	
Region	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate	EMV Cards	Adoption Rate
Africa & the Middle East	219M	74.8%	272M	87.8%	312M	89.4%
Asia Pacific	4,147M	45.7%	5,001M	51.0%	6,226M	58.1%
Canada, Latin America, and the Carribbean	820M	85.7%	848M	86.9%	923M	86.7%
Europe Zone 1	939M	84.4%	966M	85.5%	1,040M	85.9%
Europe Zone 2	276M	71.4%	301M	80.4%	318M	80.7%
United States	785M	58.5%	842M	60.7%	1,074M	60.9%

Figure 8 : Taux d'adoption par zone géographique du système EMV (Source : https://www.emvco.com/)

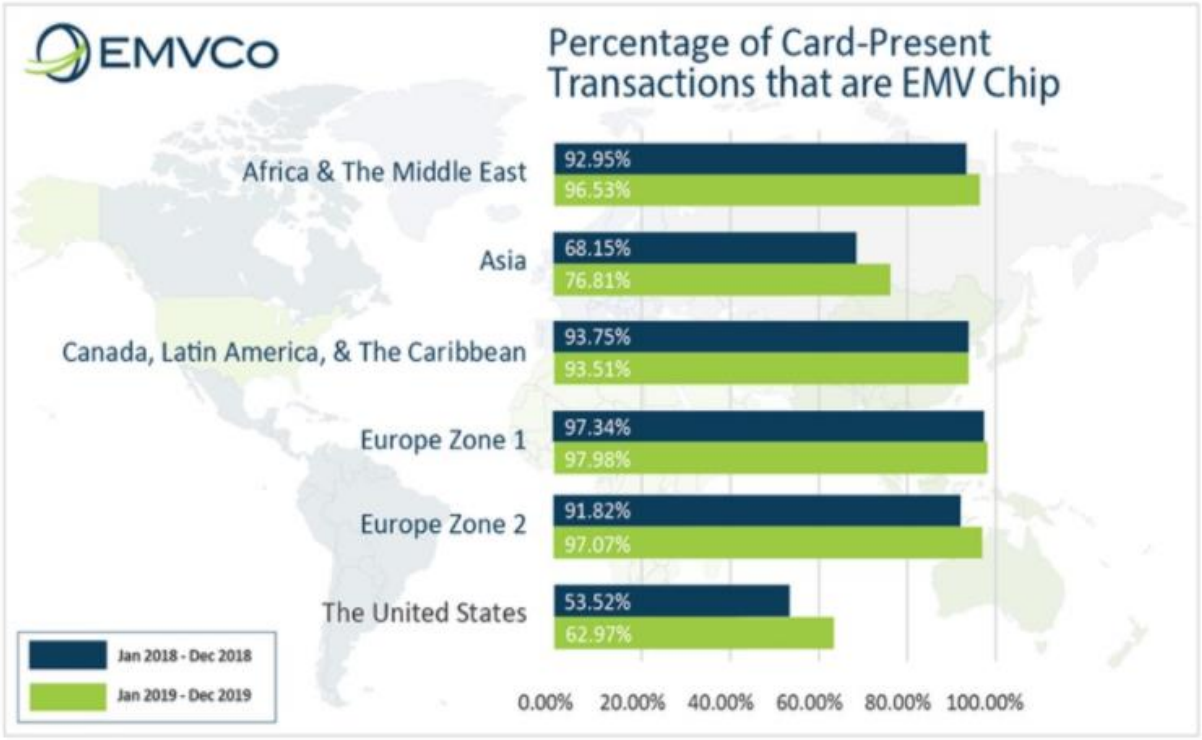


Figure 9 : Taux de transaction par zone du système EMV (Source : https://www.emvco.com/)

c) Piste magnétique

Une piste magnétique est une bande constituée de pigments magnétiques pouvant retransmettre une information binaire (qui retourne 0 ou 1).
La piste magnétique doit respecter certains standards décrits par les normes ISO :

- ISO 7811-2 : Spécifie les contraintes de la bande magnétique [7]
- ISO 7811-4 : Spécifie la position des pistes magnétiques pour lecture uniquement [8]

- ISO 7811-5 : Spécifie la position des pistes magnétiques pour lecture et écriture

Les pistes magnétiques contiennent entre autres :

- Le numéro de la carte
- La date d'expiration
- Le type de carte (débit différé, autorisation systématique, etc.)

2.4) Les terminaux de paiements

2.4.1) Historique des terminaux

Avant l'apparition des terminaux de paiement électroniques, les commerçants devaient imprimer l'information de la transaction par carte sur papier et ensuite la transmettre à la banque ; ce procédé était long et couteux.
Il faudra attendre les années 80 pour voir apparaitre les premiers terminaux de paiement électroniques lancés par VISA.

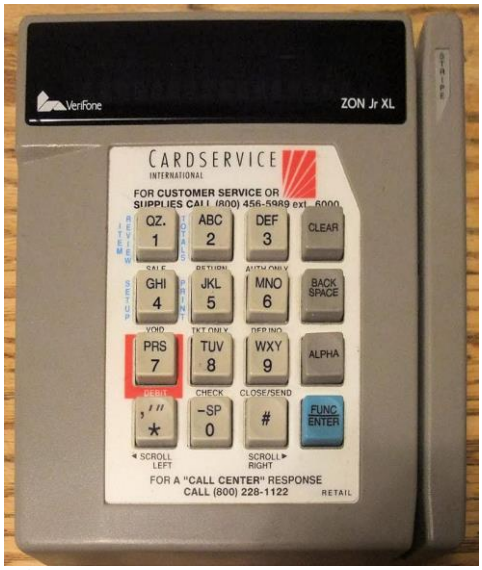


Figure 10 : ZON Jr XL, premier terminal de paiement avec autorisation (1984) (Source : https://www.mobiletransaction.org/history-of-credit-card-machines/)

Depuis, les terminaux de paiement n'ont eu de cesse d'évoluer, intégrant des interfaces sans-contact, devenant tactiles et intelligents.
Aujourd'hui, nous pouvons trouver des terminaux de paiement qui ne sont pas affiliés à des banques ; ainsi les banques ne servent plus d'interface, les frais bancaires sont donc réduits.

Figure 11 : terminal de paiement sans banque affilié (Source : https://sumup.fr/)

2.4.2) La sécurité des terminaux de paiement électroniques

Les normes de sécurité applicables aux systèmes monétiques sont aussi applicables pour le terminal de paiement et ceux-ci doivent répondre aux mêmes exigences. [9]

Un terminal de paiement doit vérifier à minima :

1. L'authentification de la carte : identifier l'appareil utilisé pour le paiement (carte bancaire avec bande magnétique, carte bancaire avec puce NFC, smartphone, etc.). Afin de se protéger contre les contrefaçons, l'authentification permet aussi de garantir la sécurité de l'information.
2. Vérification de l'utilisateur de la carte : Vérification du code pin ou de la signature entrée par le client afin de pouvoir l'identifier et éviter les fraudes liées aux vols d'appareil de paiement.
   Cette vérification ne peut pas s'appliquer pour des paiements sans contact par carte bancaire.
3. L'autorisation de paiement : Obtenir la confirmation de l'autorisation de la transaction par la banque.

2.5) Les différents types de fraudes

Les fraudes basées sur les cartes de paiement sont sans doute les plus connues puisque les plus anciennes et les plus médiatisées.
La plus simple des fraudes, et donc l'une des plus répandues, consiste à collecter les données présentes sur les pistes magnétiques d'une carte de paiement. Ces données peuvent permettre de réaliser des opérations de retrait ou de paiement.

La dotation en « puces » des cartes de paiement, qui a pour objectif de réduire ce type de fraude, a eu pour conséquence de transférer une partie de l'intérêt des fraudeurs sur cette technologie. À ce jour, seules deux fraudes ciblant les microprocesseurs sont recensées : la première visant l'espionnage des échanges entre la carte et le terminal, la seconde vise à modifier le comportement observé de la carte.

2.5.1) Skimming

La fraude par skimming permet de récupérer les données de la carte de paiement sans que l'utilisateur de celle-ci ne s'en rende compte. Le vol de ces données se fait en général lors d'une transaction légitime. Le porteur de la carte l'insère dans un terminal infecté et celui-ci récupère et envoie les informations aux fraudeurs.

La majorité des fraudes par skimming se font via l'interface magnétique de la carte.

Le nom/prénom, numéro de la carte, date d'expiration et le code de vérification de la carte est récupéré [10]

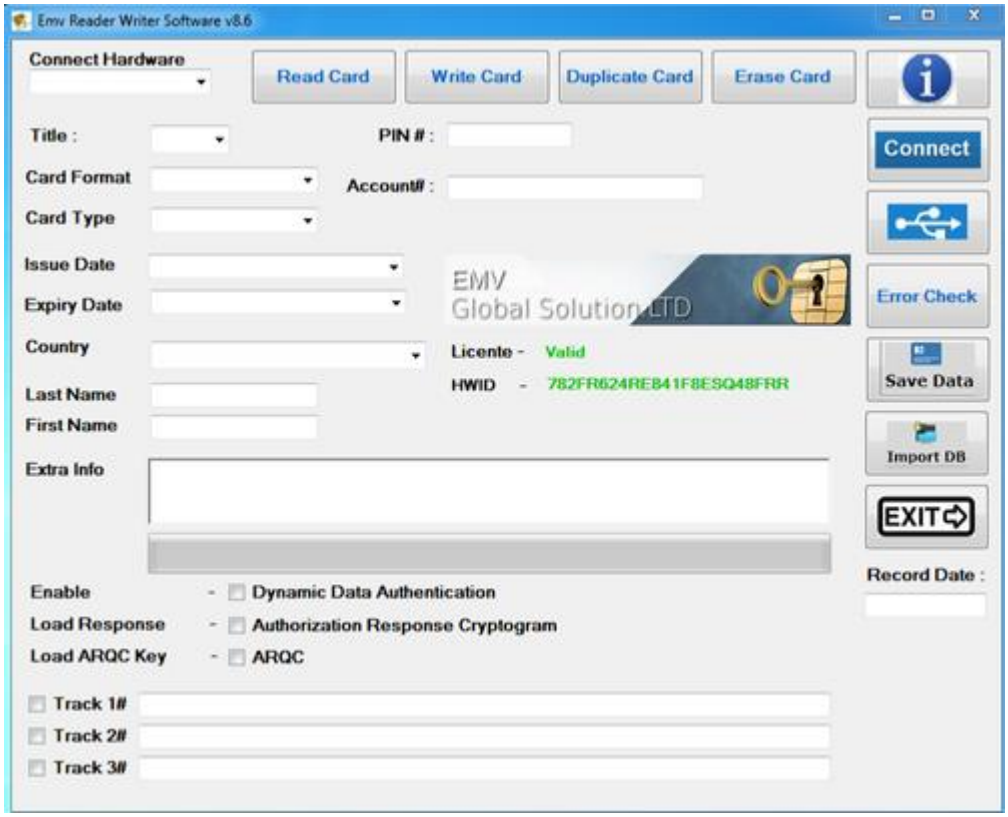


Figure 12 : Exemple de logiciel permettant de lire une carte de paiement (Source : Google)

Le fraudeur peut ensuite soit utiliser ces informations soit les revendre afin de créer une carte contrefaite.

Ce type de fraude est surtout présent en Europe, Asie et en Amérique latine.

2.5.2) Fraude par attaque de l'homme du milieu

L'attaque par l'homme du milieu (man in the middle attack) s'effectue lorsque les données de transactions sont interceptées. Par définition, cette attaque inclut une personne tierce qui de manière ponctuelle peut vous observer lorsque vous effectuez votre paiement et voler votre code de carte. Cependant, les attaques les plus élaborées permettent la mise en place de systèmes d'écoute qui permettent d'intercepter les informations entre le porteur de la carte et le marchand.
Par exemple, si un porteur de carte effectue un achat sur Internet depuis le réseau wifi non sécurisé d'un café, l'information de la transaction peut être volée et réutilisée. [11]

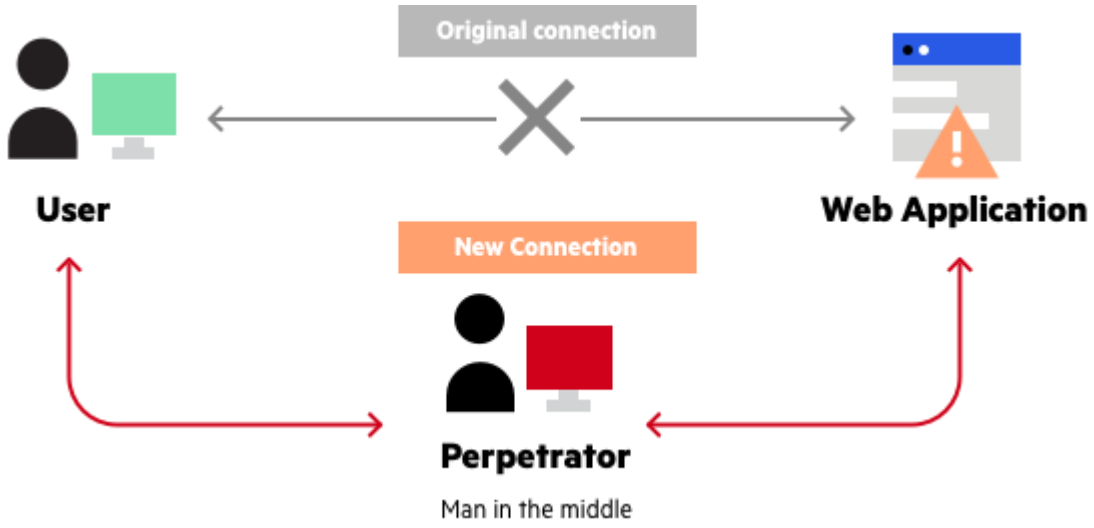


Figure 13 : Schéma d'une attaque par l'homme du milieu (Source : https://medium.com/)

2.5.3) Terminaux de paiement infectés

Les criminels se procurent un terminal pour en étudier le fonctionnement afin de pouvoir déjouer les mécanismes de sécurité. Dans certains cas, le commerçant est complice et travaille avec les pirates, il fournit ainsi le terminal aux pirates ; ceux-ci le modifient afin d'y capturer les données clients lorsque qu'ils effectuent des opérations.

Cependant, la violation d'un terminal de paiement ne nécessite plus forcément l'accès physique au dispositif de paiement. Les données peuvent être obtenues directement par intrusion sur le réseau (en LAN ou par Wifi). Les pirates commencent par balayer le réseau afin d'en identifier les terminaux vulnérables (mise à jour de sécurité obsolète, par exemple), ils exploitent ensuite les failles ou tentent une intrusion par bruteforce. Quand les pirates y ont accès, ils procèdent à l'installation d'un logiciel.

La fraude à la carte bancaire représentait en 2018 une perte de 800 millions d'euros pour les banques françaises.

2.5.4) Fraudes basées sur les terminaux

Ce type de fraude s'attaque directement aux terminaux et non plus au porteur de la carte. Il peut s'agir d'un terminal de paiement physique (DAB), virtuel ou tout autre terminal de paiement.
Les attaques peuvent soit exploiter des failles existantes dans les terminaux de paiement, soit modifier ceux-ci en y ajoutant des dispositifs permettant la récupération d'information.

2.5.5 Ingénierie sociale

Les appareils utilisés par les clients (Smartphone, Tablette, Ordinateur, Smart Watch) sont autant d'éléments à considérer lorsque l'on parle de fraude monétique. Cependant, ces éléments étant personnel à l'usager, ils sont difficilement contrôlables par les acteurs du système monétique. C'est pour cela qu'une partie des fraudes cible directement le client.

a) Phishing ou hameçonnage

La fraude par hameçonnage, ou *phishing* est l'une des fraudes les plus connues, en effet, la majorité des personnes utilisant Internet a fait l'expérience d'une tentative de phishing.

La fraude ne nécessite pas de compétences en cryptographie, ou en sécurité informatique importante.
On envoie un mail à plusieurs centaines de milliers d'utilisateurs, en usurpant l'identité d'une banque ou d'un marchand en ligne. Les mails indiquent en général un problème important sur le compte client ou une offre très alléchante pour le client. Dans les deux cas, ces objets de mail peuvent attirer le client et l'inciter à se rendre sur un site frauduleux (reprenant la charte graphique du site visé) détenu par les criminels. Le client y indique ses informations d'authentification ou de sa carte bancaire.

Le nombre de personnes qui ouvrent des mails frauduleux est assez faible (<1%) , cependant comme un grand nombre de clients sont ciblé mathématiquement les fraudeurs arrivent à toucher certains clients. Les campagnes de phishing cible un grand nombre de clients et sur une campagne d'un million de mails, on peut avoir 10 000 clients arnaqués.

De plus, le coût pour les criminels est faible (coût d'envoi de mail de masse). La multitude d'informations récupérées en fait une fraude simple, mais redoutable, les criminels peuvent par exemple contourner certaines doubles authentifications demandant une date de naissance, ou encore effectuer des demandes de modification de numéro de téléphone ou de mail auprès des banques et commerçants.

En 2020, plus de 40 millions de fraudes au phishing ont été constatées pour plusieurs centaines de millions de tentatives.

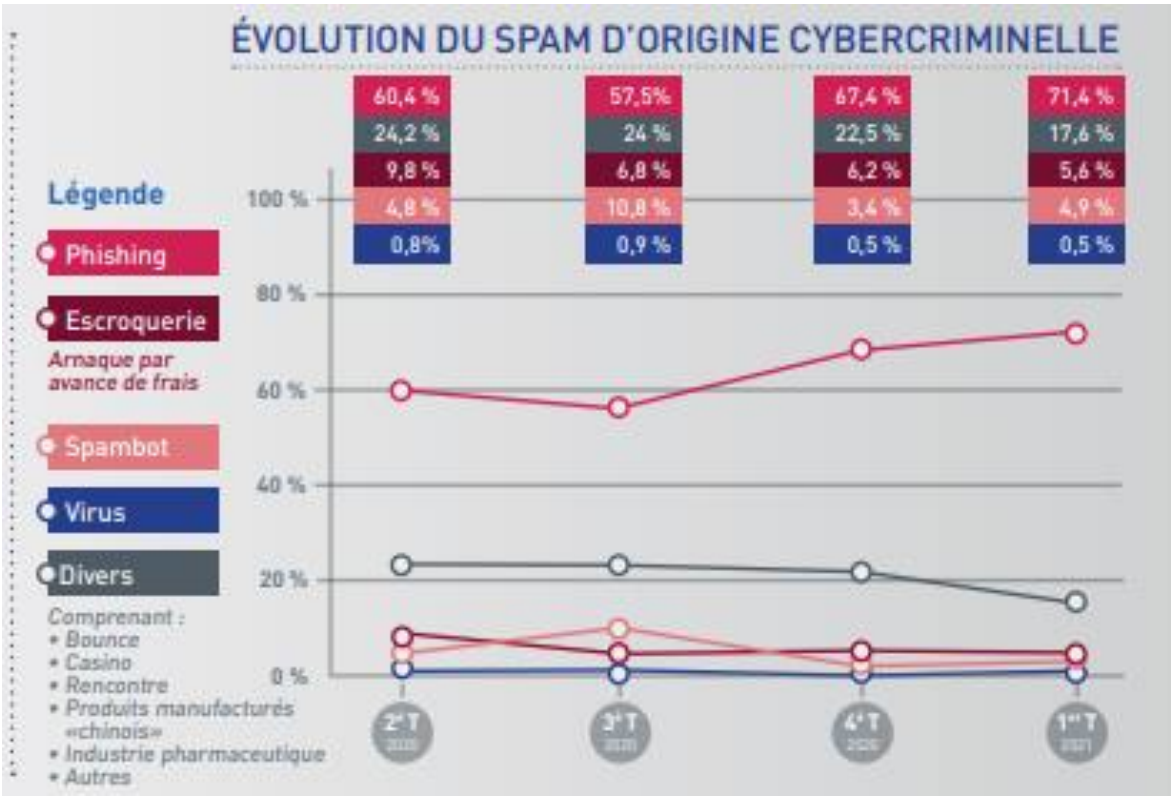


Figure 14 : Evolution du nombre de spams (Source : https://www.signal-spam.fr/)

LE TOP DES OBJETS PAR CATÉGORIE

n°	Objet par Catégorie / PHISHING	Objet par Catégorie / SCAMY	Objet par Catégorie / SPAMBOT
1	*** SPAM *** Re:	Bonjour	*** SPAM *** Votre profil est apparu cette semaine dans les résultats de 21 recherches
2	Votre colis est en route.	Hello	*** SPAM *** Réponse à votre demande du 24/11/2020
3	Hervé sent you a new message	I Have Donation For You	*** SPAM *** Covid-19
4	*** SPAM *** Notification	Re: FERMETURE DE VOTRE COMPTE *(fournisseur de messagerie)*	*** SPAM *** Notification
5	*** SPAM *** Pandemic	Bonne réception	# traking number

Figure 15 : Objets les plus courants parmi les spams (https://www.signal-spam.fr/)

Figure 16 : Exemple de mail frauduleux (Source : https://www.creditmutuel.fr/fr/particuliers/comptes/reconnaitre-phishing.html)

b) Fraude par keyloggin

La fraude par keyloggin ou logiciel espion est une fraude qui consiste à infecter un ordinateur ou un smartphone avec un logiciel malveillant. Une fois le logiciel malveillant mis en place, celui-ci va capturer les informations sécurisées de l'utilisateur (par enregistrement des touches, capture d'écran ...).
Ainsi, lors d'une double authentification, le logiciel espion pourra intercepter le SMS reçu et l'utiliser pour valider une transaction frauduleuse.

Les logiciels de keyloggin permettent de récupérer les identifiants de connexion au compte et mots de passe aux sites de banques. Certains logiciels permettent aussi de récupérer le numéro de la carte bancaire entrée chez un commerçant.

2.5.6) BruteForce

Les attaques par bruteforce ou « moulinage » en français représentent une très faible majorité des opérations frauduleuses constatées. L'attaque par bruteforce consiste à essayer sur des sites commerciaux des milliers de combinaisons pour réussir à trouver une combinaison de : numéro de carte / date d'expiration / cryptogramme. Quand une combinaison est acceptée par un site commercial alors les malfaiteurs réutilisent cette combinaison pour effectuer des achats aux sommes importantes.
Étant donné les nombreux paramètres à trouver, cette technique présente un taux de réussite assez faible.
Cependant, les nombreuses requêtes envoyées aux serveurs peuvent affaiblir les plateformes de paiements et laisser une plus grande marge à d'autres types d'attaques, notamment les attaques par déni de service (DDOS).

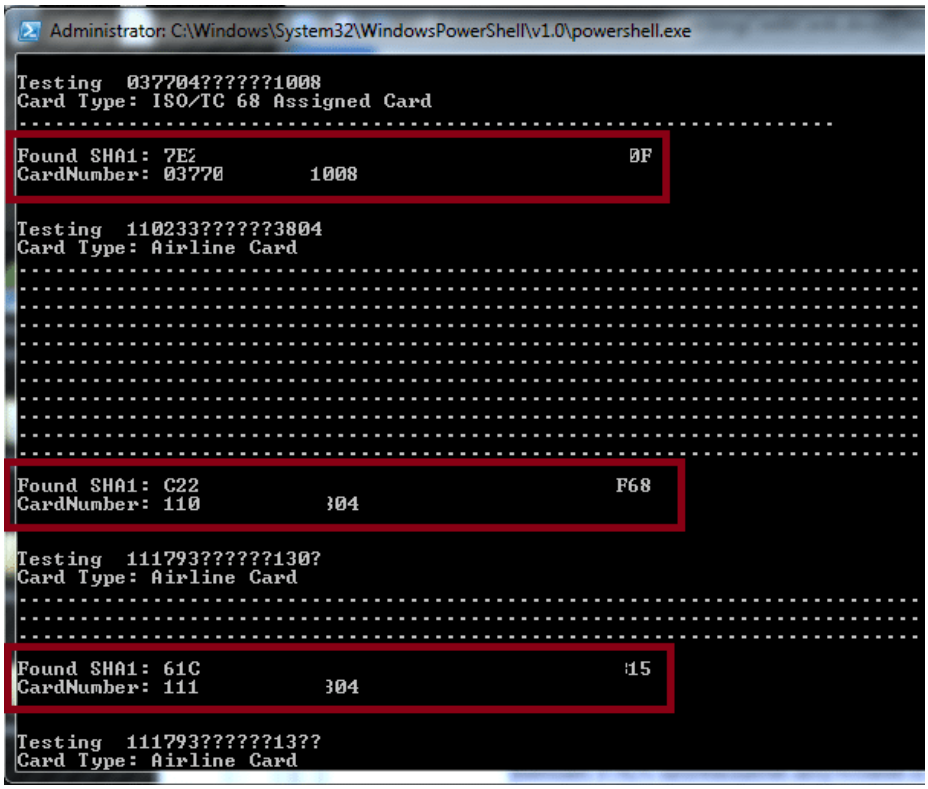


Figure 17 : Outil de bruteforce (Source : https://www.netspi.com/blog/technical/network-penetration-testing/cracking-credit-card-hashes-with-powershell/)

2.6) Le coût de la fraude

Le coût de la fraude à la carte bancaire est un sujet délicat pour les banques et les systèmes de paiements, de ce fait les chiffres (en coût et nombre) sont souvent non communiqués.

Cependant, les Banques Nationales et la BCE nous permettent d'obtenir une analyse chiffrée de la fraude monétique.
Ainsi, chaque année, la Banque de France et la BCE publient respectivement un rapport sur la fraude en France et sur la fraude dans les pays SEPA.

2.6.1) En Europe

Dans son rapport annuel, le travail effectué par la BCE nous permet de nombreux indicateurs sur la carte de paiement et sur la Fraude. On peut noter que l'utilisation et l'adoption de la carte de paiements peuvent sensiblement différer suivants les pays, par exemple, le nombre de paiements moyen par carte bancaire au Danemark est 20 fois supérieur au nombre de paiements en Bulgarie (366 vs 18).[12]

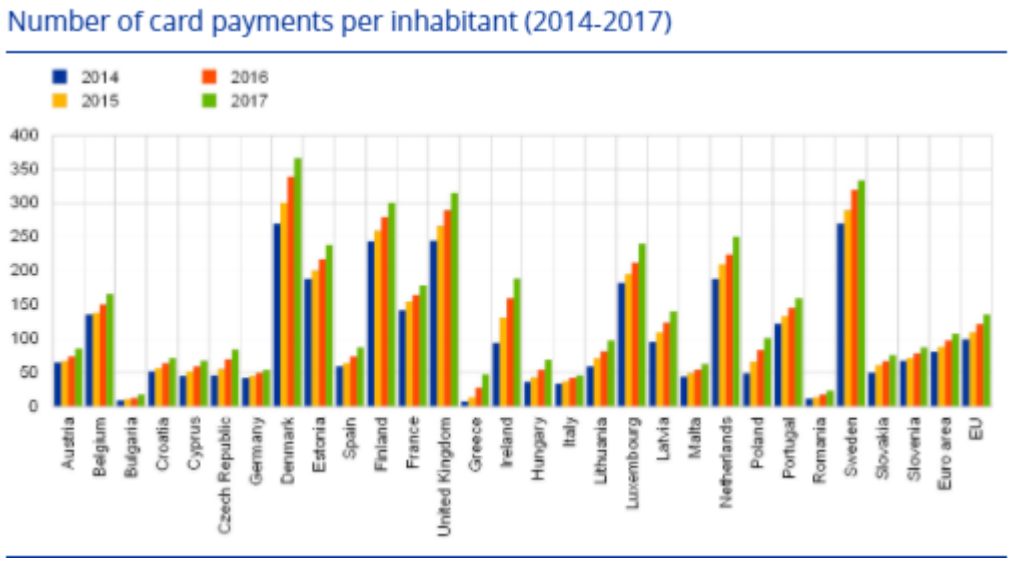


Figure 18 : Nombre de cartes de paiements par pays (Source : Sixth report on card fraud/ ECB)

En 2018, le montant des transactions effectuées par carte bancaire dans les pays SEPA s'élevait à 4,86 milliards de milliards d'euros (89,65 milliards de transactions) pour 1,80 milliard d'euros de transactions frauduleuses (21 millions de transactions).
Ces chiffres nous indiquent que la fraude ne représente qu'une infime partie des montants engagés lors de paiements par carte bancaire.

Les données de la BCE nous renforcent dans l'idée que la plupart des transactions sont des fraudes à distance (Card not present).

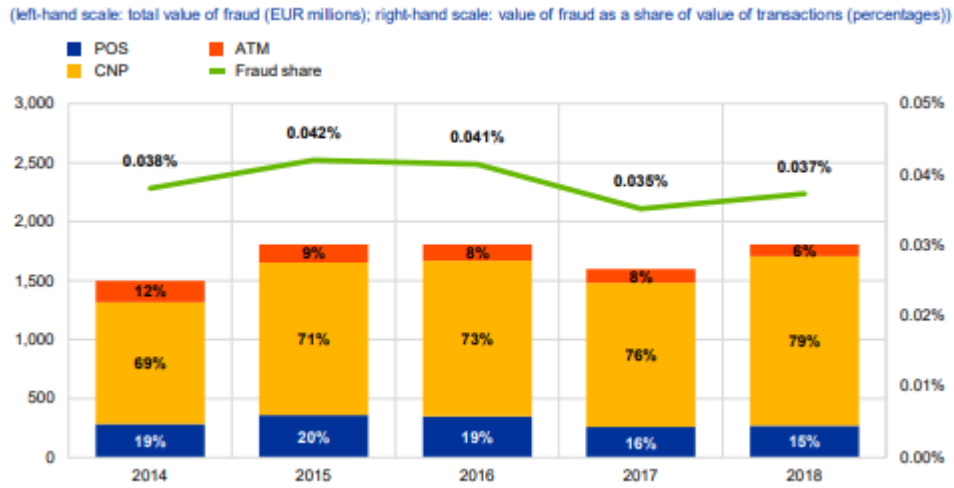
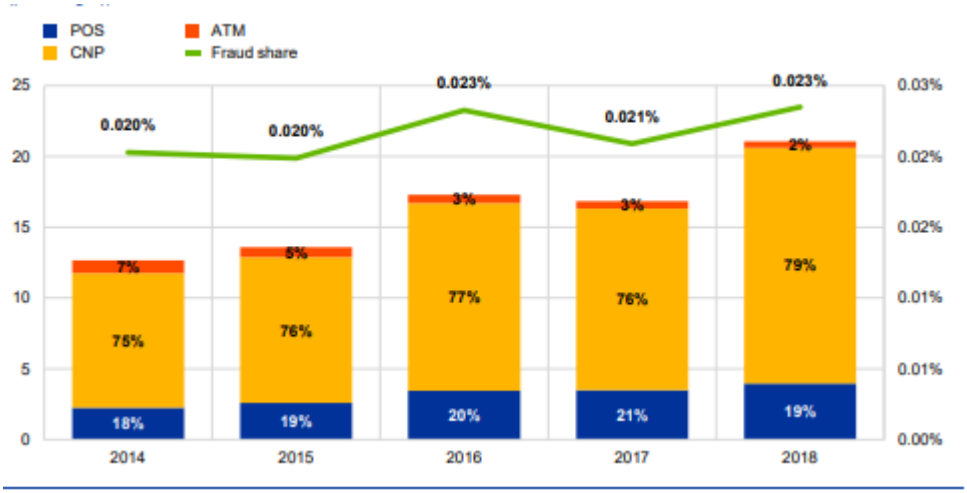


Figure 19 : Montant de la fraude & proportion des montants frauduleux vs montant des paiements non frauduleux (Source : Sixth report on card fraud/ ECB)

On observe que le montant représenté par la fraude en fonction du montant total de toutes les transactions n'a cessé de diminuer en 2015, 2016, et 2017. Une augmentation est constatée en 2018, cependant, le pourcentage reste plus bas que le niveau de 2015.
Il est à noter que les paiements à distance (CNP) représentent une part de plus en plus importante chaque année des fraudes.



Le nombre est corrélé aux montants, de ce fait l'analyse sera la même que précédemment ; on peut cependant noter que les paiements de points de retraits sont moins bien représentés (ils représentent 2% du nombre de transactions pour 6% des montants en 2018). Les fraudes aux points de retrait semblent avoir un montant moyen plus élevé.

2.6.2) En France

La carte bancaire reste en 2020 le moyen de paiement préféré des Français, ce moyen de paiement représentait 55% des paiements en 2020. Cependant, on peut noter une baisse du nombre de paiements en 2020 dû à un contexte particulier et une crise sanitaire qui a conduit à la fermeture de beaucoup d'établissements. Ainsi, les paiements de proximité étaient en baisse de 8,7% en 2020 par rapport à 2019. Parmi les paiements de proximité, on observe une augmentation du nombre paiement sans contact, ceux-ci étant recommandés dans le contexte, on peut aussi noter l'augmentation du plafond de paiement, passant de 30 à 50€.

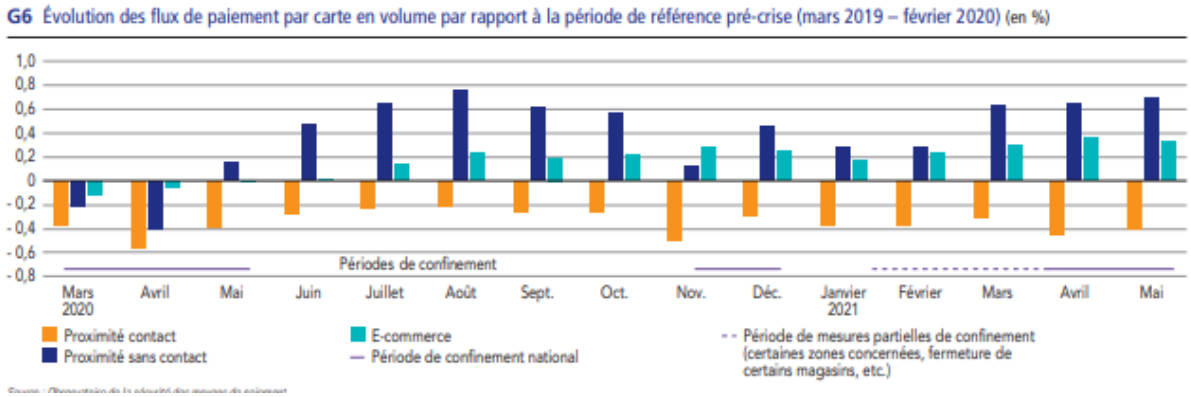


Figure 20 : Evolution des flux de paiement précovid vs covid (Source : Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2020)

En 2020 la carte de paiement représentait 95% des transactions frauduleuses (2,8% pour le chèque, 0,5% pour le virement, 0,1% pour le prélèvement, et 1,5% pour les retraits carte)
Le taux de fraude reste relativement faible (0,068%) comparé à d'autres moyens de paiement comme le chèque (0,088%). On note tout de même une légère augmentation, le taux de fraude sur la carte bancaire était de 0,064% en 2019.

On observe une augmentation du montant fraudé sur les paiements à distance (+ 16,4%) et une diminution du montant fraudé pour les paiements de proximité.
Il est difficile de tirer des conclusions de ces chiffres, car ils sont fortement corrélés à la dynamique due au covid-19. [13]

2.7) Les différents leviers de lutte contre la fraude monétique

2.7.1) DSP2

En 2015, la directive européenne sur les services de paiement est adoptée par le Parlement européen. L'une des principales dispositions de la directive est la disposition sur les services de paiements, ainsi : « les prestataires de services de paiement devront adopter des technologies assurant une **authentification forte du client** lorsqu'elle est requise et veiller à ce que les données de sécurité de l'utilisateur soient transmises par des canaux sûrs » [15].

Cette directive est entrée en vigueur en septembre 2019, mais avec une applicative progressive.
Depuis le 15 mai 2021, tous les paiements peuvent faire l'objet d'une authentification forte.

L'authentification forte correspond à une authentification du client à deux étapes, le client devra s'authentifier avec au moins 2 des moyens ci-dessous :

- Un de mot de passe personnel
- Un appareil personnel
- Une reconnaissance biométrique (digitale, vocale ou faciale)

2.7.2) Les acteurs institutionnels

L'État français a mis en place plusieurs actions afin de lutter contre la fraude monétique, il a mis en place via la banque de France un organe chargé de cette mission l'observatoire de Sécurité des Moyens de paiement (OSMP). L'OSMP a 3 missions : «

- Il assure le suivi de la mise en œuvre des mesures adoptées par les émetteurs, les commerçants et les entreprises pour **renforcer la sécurité des moyens de paiement** ;
- Il **est chargé d'établir des statistiques en matière de fraude**. À cette fin, les émetteurs de moyens de paiement adressent au secrétariat de l'Observatoire les informations nécessaires à l'établissement de ces statistiques. L'Observatoire émet des recommandations afin d'harmoniser les modalités de calcul de la fraude sur les différents moyens de paiement scripturaux ;
- Il **assure une veille technologique en matière de moyens de paiement scripturaux**, avec pour objet de proposer des moyens de lutter contre les atteintes à la sécurité des moyens de paiement. À cette fin, il collecte les informations disponibles de nature à renforcer la sécurité des moyens de paiement et les met à la disposition de ses membres. Il organise un échange d'informations entre ses membres dans le respect de la confidentialité de certaines informations. »[14]

2.7.3) Individuel

Les porteurs de carte de paiements ont un rôle important dans la lutte contre la fraude monétique, en effet, les fraudeurs redoublent d'ingéniosité pour contourner les moyens mis en place pour lutter contre la fraude.
La vigilance des porteurs influent directement sur la sécurité des paiements ainsi l'OSMP a émis plusieurs recommandations :

« • Lorsque vous composez un code ou un mot de passe confidentiel, veillez à le faire à l'abri des regards indiscrets. N'hésitez pas en particulier à cacher le clavier du terminal, du distributeur ou du téléphone avec votre autre main.

• Vérifiez régulièrement et attentivement vos relevés de compte.

• Pensez à consulter régulièrement les consignes de sécurité publiées sur le site de votre banque et assurez-vous qu'elle dispose de vos coordonnées afin de vous contacter rapidement en cas d'opérations douteuses sur votre compte. En cas de contact de votre banque, par téléphone ou par courriel pour de telles opérations, rappelez-vous que vous n'avez pas à lui communiquer vos mots de passe et identifiants personnels.

• N'acceptez jamais de payer un vendeur ou loueur de biens que vous ne connaissez pas par transfert d'argent préalable à la mise à disposition ou la livraison du bien. Il peut s'agir de fraudeurs qui, après avoir récupéré les fonds transférés, font disparaître tout lien de communication (adresse e-mail, compte de réseau social, etc.).
Vos instruments de paiement sur support matériel, tels que votre carte ou votre chéquier, sont strictement personnels : ne les prêtez à personne, pas même à vos proches. Vérifiez régulièrement qu'ils sont en votre possession et conservez-les en lieu sûr, si possible séparément de vos pièces d'identité.

• Si l'utilisation du moyen de paiement nécessite l'utilisation d'un identifiant confidentiel (code confidentiel pour une carte, mot de passe pour le paiement par téléphone mobile, etc.), gardez-le secret,

ne le communiquez à personne. Apprenez-le par cœur, évitez de le noter, et à défaut ne le conservez jamais avec le moyen de paiement correspondant ou de sorte qu'un lien puisse être établi avec lui. »

L'intelligence artificielle pour détecter les fraudes

Au cours des dernières années, l'intelligence artificielle est de plus en plus utilisée dans la lutte contre la fraude monétique.
Les techniques de machine Learning fonctionnent souvent de la même manière : on met en entrée plusieurs paramètres et nous avons en sorti un résultat.

Exemples :

X	Y
emails	Spam (oui/non)
Profil client	Nombre de clicks
Expression génique	État du patient
Profil électeur	Vote
Age, expérience	Salaire

Figure 21: Fonctionnement simplifié d'un modèle de machine Learning

Les arbres de décisions et forêts aléatoires :

Principe : réfléchir dimension par dimension, probablement le plus proche d'une décision humaine.

Les arbres s'utilisent dans des problèmes de régression et de classification.
Ils acceptent les données de types différents : qualitatives/quantitatives, discrètes/continues.
Ils sont très facilement interprétables.

Variable qualitative : Il s'agit de variables qualitatives, qui ne mesurent pas une quantité, mais évaluent un état, un statut, une catégorie.

Vocabulaire :

Nœud : endroit de coupure.
Racine : nœud initial, aucune coupure n'a été faite.

Feuille : extrémité de l'arbre (nœud qui n'est pas divisé).
Profondeur : nombre de niveaux de l'arbre
Taille minimale des feuilles : nombre minimal de points de l'ensemble d'apprentissages toléré dans une feuille.
Critère de séparation : critère selon lequel on choisit la variable/la coupure.

Fonctionnement : Les arbres de décisions sont des constructions hiérarchiques avec une racine, des branches et des nœuds, à partir de chaque nœud partent 2 branches et rejoignent d'autres nœuds.
Une fois toute les coupures effectuées, et qu'il ne reste que des feuilles, les données des individus aux feuilles sont utilisées pour de la prédiction. [16]

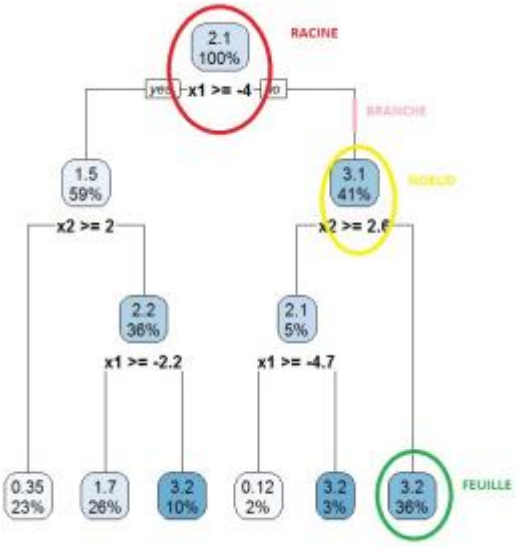


Figure 22: Exemple d'arbre de décision (Source A. Teixeira)

2.8) Présentation de la démarche

2.8.1) Diagnostic

Lorsque qu'une fraude est avérée, le remboursement du client peut s'effectuer soit par la banque elle-même (le coût sera alors pris en perte dans le bilan), soit le dossier sera envoyé au prestataire gérant la carte bancaire afin qu'il puisse recouvrir les fonds et émettre le remboursement. Il est à noter que lorsqu'un dossier frauduleux est envoyé aux prestataires, celui-ci facture [redacted]€ de frais de recherche à la banque. De ce fait, si le montant d'une fraude est inférieur à [redacted]€, celui-ci sera pris en charge par la banque, autrement, il sera envoyé chez le prestataire.
En 2020, [redacted]% des pertes du service monétique étaient dus au remboursement de la fraude.

Le coût de la fraude monétique n'est pas négligeable chez BforBank, ainsi sur l'année 2020, [redacted]€ ont été pris à perte.

En 2020 [redacted]% des fraudes étaient faites sur de la vente à distance et [redacted]% d'entre elles passaient par le réseau CB (réseau domestique).

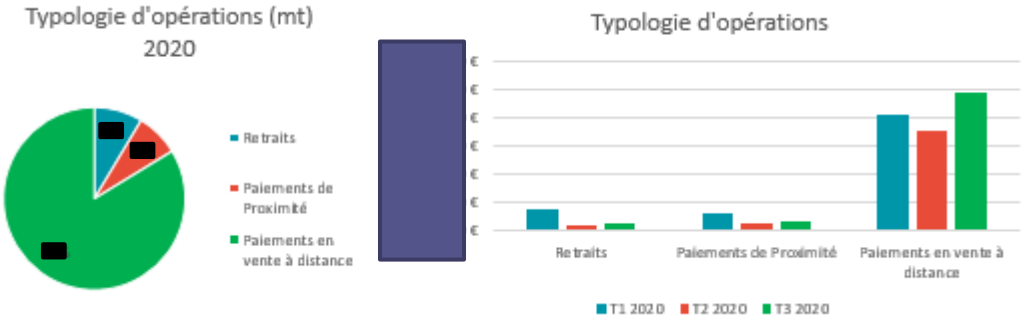


Figure 23 : Evolution du montant de la fraude sur l'année 2020 chez BforBank (Source : Interne)

2.8.2) Identification des points à traiter, orientation

Aujourd'hui, plusieurs axes d'amélioration sont à l'étude notamment :

- Une digitalisation du traitement des fraudes monétiques
  - Le traitement et la remontée de données sont effectués sur Excel, ce qui n'est pas l'outil le plus efficace pour des traitements de fraude monétique
  - De plus, ce système ne permet pas une remontée des données dans notre DataWare House, ce qui complique la tâche du Pole Data-Science & Analytics dans ses missions
  - Le traitement des fraudes monétiques est réalisé manuellement
  - Ce traitement manuel entraine des erreurs et donc une plus grande difficulté lors de la réconciliation des données
- Une revue de la tarification des dossiers auprès de notre prestataire Monext

- Une revue des seuils d'Alertes Fraudes
    - Les seuils actuels ne sont pas efficients, un trop grand nombre d'alertes sont générées par rapport à la fraude effective (Plusieurs dizaines de milliers par mois), et bien souvent, les fraudes se trouvent en dessous du seuil fixé.
    - La revue de ces seuils doit être faite rapidement, car en plus du manque de pertinence, ces alertes génèrent de l'insatisfaction client (de nombreux SMS reçus pour un même client), et un coût pour BforBank ([redacted]cts par SMS, soit [redacted] € par mois en moyenne).

3) Étude de cas

Dans cette partie, nous chercherons à démontrer qu'un traitement par algorithme de la détection de la fraude peut être pertinent.
Pour ce faire, nous allons élaborer un modèle basé sur des fraudes déjà identifiées.

3 .1) Construction de notre base d'étude

La construction de la base d'études est un élément clé du scoring ainsi que l'étape la plus longue. Durant cette étape, nous allons définir l'événement à étudier, ainsi que la population à étudier.

Il faut être très vigilant durant cette étape, car le choix de l'événement à étudier et la population cible va influer directement sur la performance de notre modèle.

Comme évoqué dans le paragraphe précédent, le service monétique nous a fourni une base de données non exhaustive des transactions frauduleuses.

Ces données étant issues d'un traitement manuel, elles ne possèdent pas d'identifiant unique nous permettant de les retrouver dans nos bases de données, nous avons donc dû procéder à une réconciliation à partir d'éléments fournis dans cette base de données initiale.

Pour retrouver les opérations frauduleuses dans nos bases de données, nous avons réconcilié les données par :

- Montant de l'opération
- Numéro de la carte bancaire utilisé
- Date de la transaction

Sur les 40 000 transactions fournies par le middle-office monétique, 10 581 ont pu être réconciliées, nous nommerons ces transactions jeu de données F. La perte est importante,

cependant, la réconciliation est essentielle, elle nous permettra de trouver de nouveaux indicateurs contenus dans nos bases de données.
Cette perte s'explique par des erreurs humaines par exemple en employé du MO va se tromper entre la date d'achat et la date d'enregistrement par le système de paiement, inverser les chiffres sur le montant etc.

Cela a un impact important étant donné que nous aurons 30 000 transactions frauduleuses dans notre base non identifiée et donc « légitime » dans le jeu de donnée.

Pour créer un modèle de détection des fraudes à la carte bancaire, il nous faut bien évidemment un échantillon de transactions frauduleuses, mais aussi un échantillon de transactions non frauduleuses ou non détectées.

Pour créer cette base d'études contenant à la fois les transactions frauduleuses et non frauduleuses, nous allons partir de toutes les opérations effectuées entre 2015 et 2020 (environ 70 M d'enregistrements), nous appellerons ce jeu de données A. Depuis le jeu de données A, nous allons créer un jeu de données excluant toutes les cartes ayant eu au moins une transaction frauduleuse que nous nommerons jeu de données B et un autre échantillon contenant toutes les cartes ayant eu au moins une transaction frauduleuse que nous nommerons C. De fait, le jeu de données C contient F.

L'échantillon B étant trop volumineux pour nos capacités d'analyse, nous effectuons donc un échantillonnage de ce jeu de donnée. Nous sélectionnerons toutes les transactions de 2500 cartes tirées aléatoirement. Ce sera notre échantillon D.

Nous avons donc 5 jeux de données :

- L'échantillon F contenant toutes les transactions frauduleuses
- L'échantillon A contenant toutes les transactions entre 2015 et 2020 (Volumétrie : 70M)
- L'échantillon B contenant les transactions sans aucune des cartes bancaires identifiées comme frauduleuses (69M)
- L'échantillon C contenant les transactions avec des cartes bancaires identifiées comme frauduleuses (1M)
- L'échantillon D, sous-ensemble de B

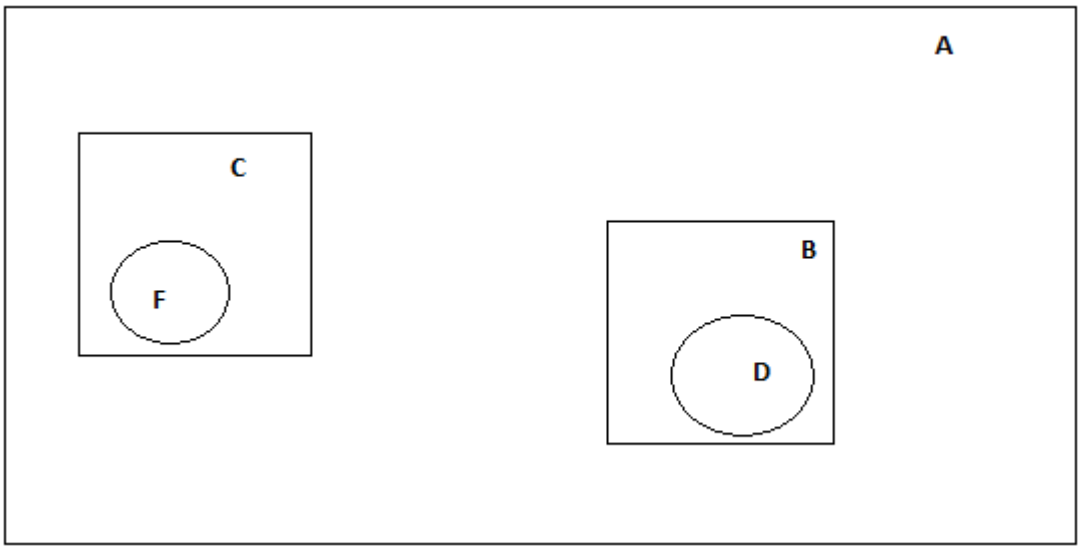


Figure 24 : Schéma du dataset (Source : Interne)

Dans le cadre de notre étude nous allons utiliser toutes les transactions présentes dans C et D.

3.1.1) Variable primaire

Dans les jeux de données nouvellement créés, nous disposons de plusieurs variables :

Variable	Description
FRAUDE	Indicateur de fraude
CARTE_TYPE	Indique la gamme de la carte utilisée
FTTC_CUSTOMER	Permet d'identifier le type de transaction (paiement de proximité, paiement web, hors Europe…)
RAISON_SOCIALE	Raison sociale du marchand
CODE_DEPARTEMENT	Département du marchand
CODE_PAYS	Code pays de marchand
LOCALISATION	Localisation du marchand (Ville)
CODE_SIRET	Numéro Siret du marchand
LIBELLE	Libelle de la transaction
MNT_BRUT	Montant brut de la transaction
FT_BRUT_REF	Identifiant unique de transaction
CODE_MCC	Permet d'identifier le type d'activité du commerçant
Age	Âge du client
DATE_VALEUR	Date de la transaction

3.1.2) Variable secondaire
À partir de ces variables, nous pouvons créer de nouvelles variables :

Variable	Description
country	Pays de la transaction recalculé
type pays	Indique si le pays de transaction est en France dans une zone SEPA ou à l'international
NB_JOUR_FTTC_CUSTOMER	Nombre de jours passés entre la transaction effectuée et la dernière transaction avec le même code de transaction
NB_JOUR_CODE_SIRET	Nombre de jours passés entre la transaction effectuée et la dernière transaction avec le même code de Siret
NB_JOUR_CODE_MCC	Nombre de jours passés entre la transaction effectuée et la dernière transaction avec le même code marchand
NB_JOUR_TYPE_PAYS	Nombre de jours passés entre la transaction effectuée et la dernière transaction dans le même type de zone (SEPA/France/International)
NB_JOUR_COUNTRY	Nombre de jours passés entre la transaction effectuée et la dernière transaction dans le même pays
MOYENNE_MONTANT_TRANSACTION_30J	Somme du montant des transactions sur les 30 derniers jours pour une carte divisée par le nombre de transactions
MOYENNE_MONTANT_J_30J	Somme du montant des transactions sur les 30 derniers jours pour une carte divisée par 30
MOYENNE_MONTANT_3_MOIS_WEEK	Somme des montants des transactions sur les 90 derniers jours divisés par 12
NB_TRANSACTION_SAME_DAY	Nombre de transactions avec la même carte effectuées le même jour
MNT_TRANSACTION_SAME_DAY	Montant des transactions le même jour
NB_TRANSACTION_SAME_MCC_30D	Nombre de transactions avec le même code marchand sur les 30 derniers jours
MNT_TRANSACTION_SAME_MCC_30D	Somme du montant des transactions sur les 30 derniers jours ayant le même code marchand divisé par 30
NB_TRANSACTION_SAME_MERCH_30D	Nombre de transactions avec le même code marchand sur les 30 derniers jours
MNT_TRANSACTION_SAME_MERCH_30D	Somme du montant des transactions sur les 30 derniers jours ayant le même code marchand divisé par 30
NB_TRANSACTION_SAME_FTTC_30D	Nombre de transactions avec le même code transaction sur les 30 derniers jours
MNT_TRANSACTION_SAME_FTTC_30D	Somme du montant des transactions sur les 30 derniers jours ayant le même code transaction divisée par 30
NB_TRANSACTION_SAME_PAYS	Nombre de transactions dans le même pays sur les 30 derniers jours
MNT_TRANSACTION_SAME_PAYS	Somme du montant des transactions sur les 30 derniers jours dans le même pays divisé par 30
NB_TRANSACTION_SAME_ZONE	Nombre de transactions dans la même zone sur les 30 derniers jours
MNT_TRANSACTION_SAME_ZONE	Somme du montant des transactions sur les 30 derniers jours dans la même zone divisée par 30
DOUBLE_MOYENNE_MNT_30J	Indique si le montant brut est 2 fois supérieur à la moyenne des paiements sur 30j
T_PERCT_MONTANT	Indique si le montant brut est inférieur à 10% du montant brut moyen sur 30j
groupe_mcc	Regroupe de code Marchand par secteur d'activité
NUM_DEP	Département de résidence du client
SALAIRE	Salaire du client

Ces variables ont été créées en se basant sur la littérature et l'expérience [10], elles correspondent notamment au critère de RFM (Recency, Frequency, Monetary), souvent utilisé dans le domaine de la fraude à la carte bancaire. [17]

3.1.3) Undersampling

Le taux de fraude dans notre base déjà réduite de bon nombre de transactions est très faible (0.65%), les techniques actuelles de Machine Learning s'adaptent mal à des jeux de données très inégaux. [17]

Plusieurs techniques existent afin d'équilibrer les jeux de données inégaux, l'oversampling par clustérisations en est une ou encore la méthode smote.

Cependant, plusieurs études indiquent que des méthodes simples d'oversampling ou d'undersampling obtiennent de meilleures performances.
Nous avons donc créé un sous-échantillon contenant 10% de fraude pour notre analyse.

3.2) Analyse de la distribution des variables

Dans cette partie, nous nous attacherons à analyser la distribution des variables et leurs relations avec la variable cible (fraude). Pour des besoins de lisibilité, seules les variables avec un lien qui semble pertinent seront analysées dans cette partie, toutes les autres analyses graphiques pourront être trouvées en annexe.

Stat/Var	FRAUDE	MNT_BRUT	NB_JOUR_FTTC_CUSTOMER	NB_JOUR_CODE_SIRET	NB_JOUR_CODE_MCC	NB_JOUR_TYPE_PAYS	NB_JOUR_COUNTRY	MOYENNE_MONTANT_TRANSACTION_30J
mean	0.1	49.6	29.4	431.6	175.3	11.6	26.5	47.7
std	0.3	108.0	157.1	513.2	370.0	95.7	157.0	48.3
min	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
25%	0.0	10.0	0.0	7.0	2.0	0.0	0.0	27.9
50%	0.0	23.0	1.0	49.0	11.0	0.0	0.0	38.8
75%	0.0	50.8	4.0	1095.0	58.0	2.0	2.0	55.3
max	1.0	8463.0	1095.0	1095.0	1095.0	1095.0	1095.0	8463.0

Stat/Var	MOYENNE MONTANT J 30J	MOYENNE MONTANT 3 MOIS WEEK	NB TRANSACTION SAME DAY	MNT TRANSACTION SAME DAY	NB TRANSACTION SAME MCC 30D	MNT TRANSACTION SAME MCC 30D	NB TRANSACTION SAME MERCH 30D	MNT TRANSACTION SAME MERCH 30D
mean	52.1	332.8	4.0	180.1	2.9	5.8	2.9	4.1
std	41.8	252.7	4.5	300.7	4.4	10.0	4.4	8.6

min	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
25%	24.5	156.4	2.0	38.2	1.0	1.0	1.0	0.6
50%	43.7	289.2	3.0	92.0	1.0	2.7	1.0	1.5
75%	68.3	447.1	5.0	201.4	3.0	6.7	3.0	3.9
max	599.2	2737.0	152.0	8463.0	101.0	282.1	101.0	282.1

Stat/Var	NB TRANSACTION SAME FTTC 30D	MNT TRANSACTION SAME FTTC 30D	NB TRANSACTION SAME PAYS	MNT TRANSACTION SAME PAYS	NB TRANSACTION SAME ZONE	MNT TRANSACTION SAME ZONE	DOUBLE MOYENNE MNT 30J	T PERCT MONTANT	SALAIRE
mean	20.2	24€	31.0	42€	31.2	43€	0.1	0.1	3557€
STD	17.8	22€	22.6	37€	22.5	37€	0.3	0.3	13147€
min	0.0	0.0€	0.0	0€	0.0	0€	0.0	0.0	0.0€
25%	6.0	8.0€	14.0	16€	14.0	17€	0.0	0.0	1829€
50%	16.0	19.0€	27.0	35€	28.0	35€	0.0	0.0	2519€
75%	30.0	33.8€	44.0	58€	44.0	58€	0.0	0.0	3688€
max	167.0	334.1€	211.0	505€	211.0	505€	1.0	1.0	523236€

En analysant les écarts-types (variable STD) dans le tableau ci-dessus, on observe que beaucoup de variables sont assez dispersées autour de la moyenne. Cela peut nous indiquer la présence de valeurs aberrantes, dites outliers.

Pour rappel : l'écart-type est la racine carrée de la variance, avec la variance égale à :

$$V = \frac{1}{n}\sum_{i=1}^{n}(x_i - \overline{x})^2.$$

Les outliers sont des valeurs qui sortent du lot (supérieur au Q3 ou inférieur au Q1), elles peuvent représenter des individus (transactions ici) atypiques ou des erreurs de mesure. Dans notre cas, les données concernant les transactions sont fiables, il ne serait donc pas judicieux de les supprimer ou de les remplacer par des valeurs proches (remplacement par la moyenne ou par imputation multiple).

Exemple de box plot de l'âge des clients ayant effectué une transaction dans le périmètre :

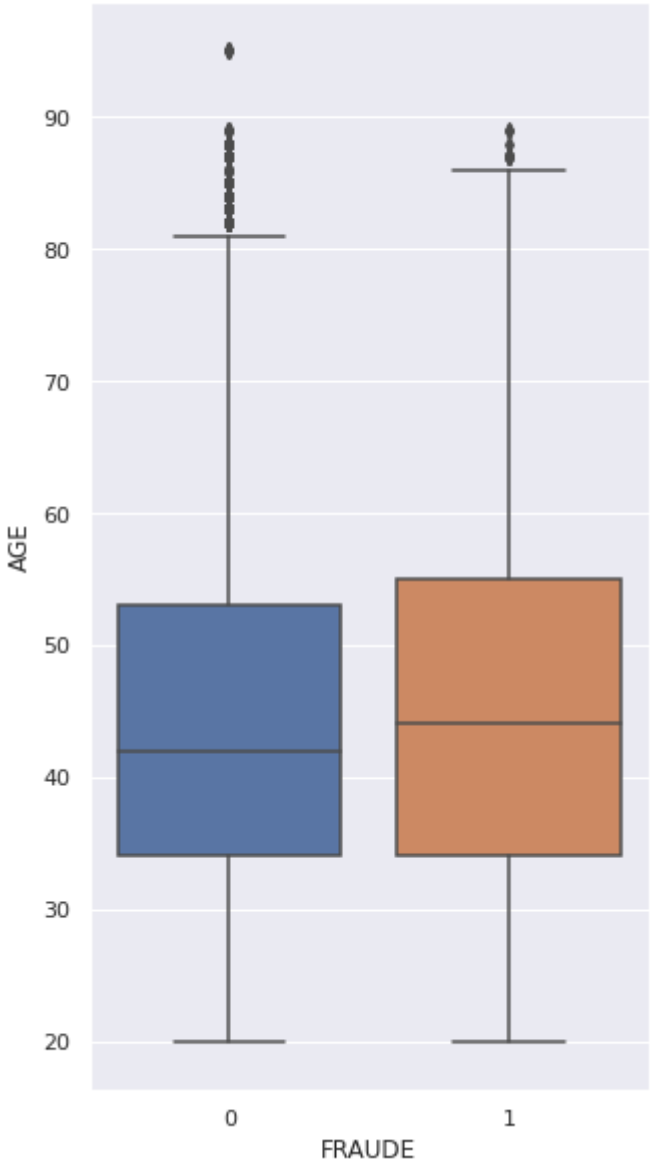


Figure 25 : Box plot de l'âge (Source : Interne)

3.2.1) Distribution du nombre de transactions avec le même code marchand durant les 30 derniers jours

Figure 26 : Montant moyen de transaction sur 30 jours effectuée chez le même type de marchand (Source : Interne)

On constate que le nombre de transactions moyen sur 30j est plus important parmi les transactions frauduleuses que parmi celles non frauduleuses.

La médiane du nombre de transactions avec le même code marchand parmi les transactions frauduleuses est 2 fois supérieure aux transactions non frauduleuses (5.2 vs 2.7)

3.2.2) Distribution du nombre et du montant moyen par mois des transactions avec le même code Siret

Figure 27 : Nombre moyen de transactions sur 30 jours effectuées chez le même type de marchand (Source : Interne)

Il est intéressant de noter que l'on obtient quasiment les mêmes graphiques qu'avec le montant moyen par type de marchand, on peut soupçonner une forte corrélation entre ces 2 variables.

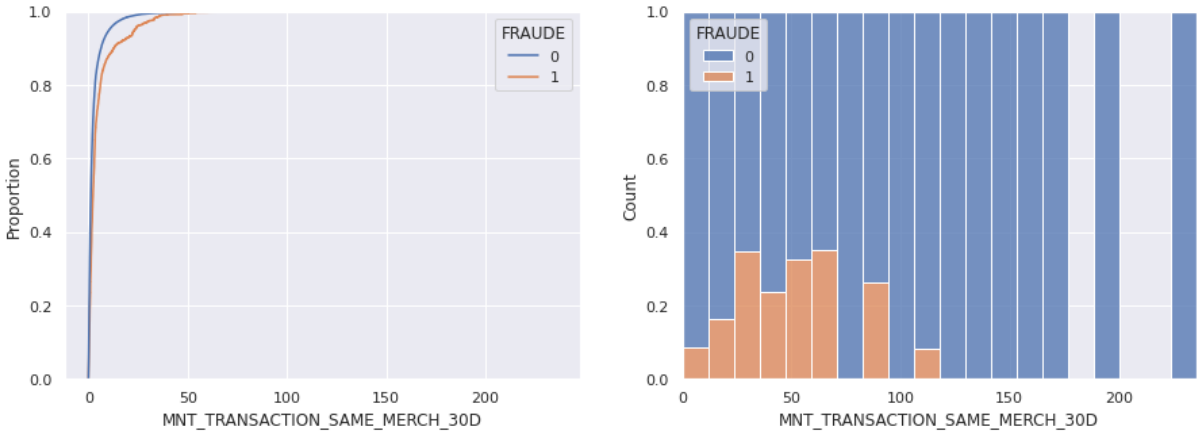


Figure 28 : Montant moyen de transactions sur 30 jours effectuées chez le même marchand (Source : Interne)

Un marchand aura toujours le même code marchand et donc le montant par marchand et par code marchand peut être égal.

3.2.3) Distribution du nombre de jours entre 2 transactions effectuées dans un même pays

Cette variable compte le nombre de jours entre 2 transactions effectuées dans un même pays, si un client n'a effectué aucune autre transaction dans le même pays que la transaction analysée alors la variable est égale à « NaN » Not a Number. Il s'agit là d'une variable dans laquelle l'évènement peut ne jamais se produire. C'est un problème bien connu dans l'analyse de survie par exemple.
Nous avons donc décidé d'appliquer une censure à droite, c'est-à-dire que le nombre de jours dépasse 3 ans (1050 jours exactement) ou que le nombre de jours est égal à NaN alors le nombre de jours sera 1050.

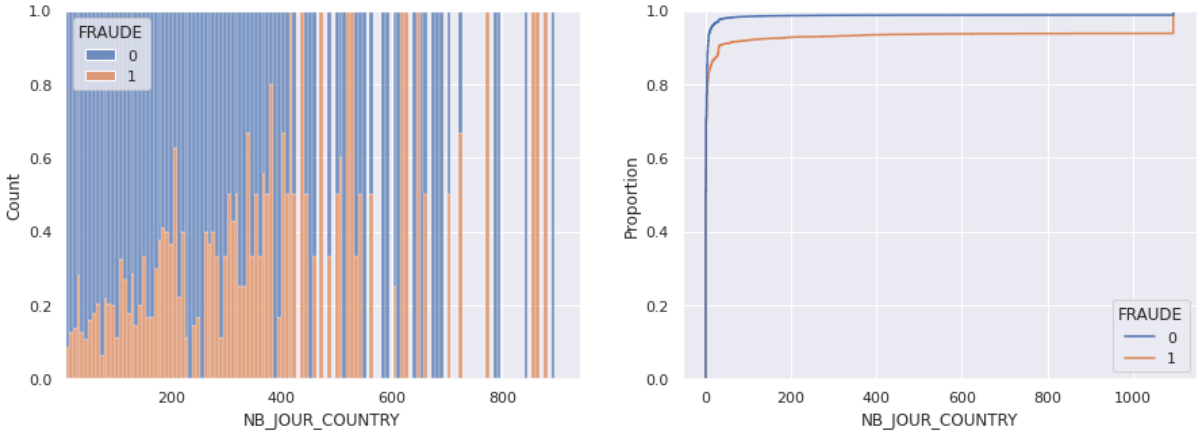


Figure 29 : Nombre de jours passé entre 2 transactions dans le même pays (Source : Interne)

Une relation quasiment linéaire semble se présenter entre le nombre de jours et l'apparition d'une fraude, plus le client a l'habitude d'effectuer une transaction dans le même pays, plus la probabilité que la transaction soit frauduleuse est faible.

Le nombre de jours moyen entre 2 transactions pour une transaction légitime est de [redacted] jours contre [redacted] jours pour une transaction frauduleuse.

3.2.4) Distribution du nombre de transactions frauduleuses par pays

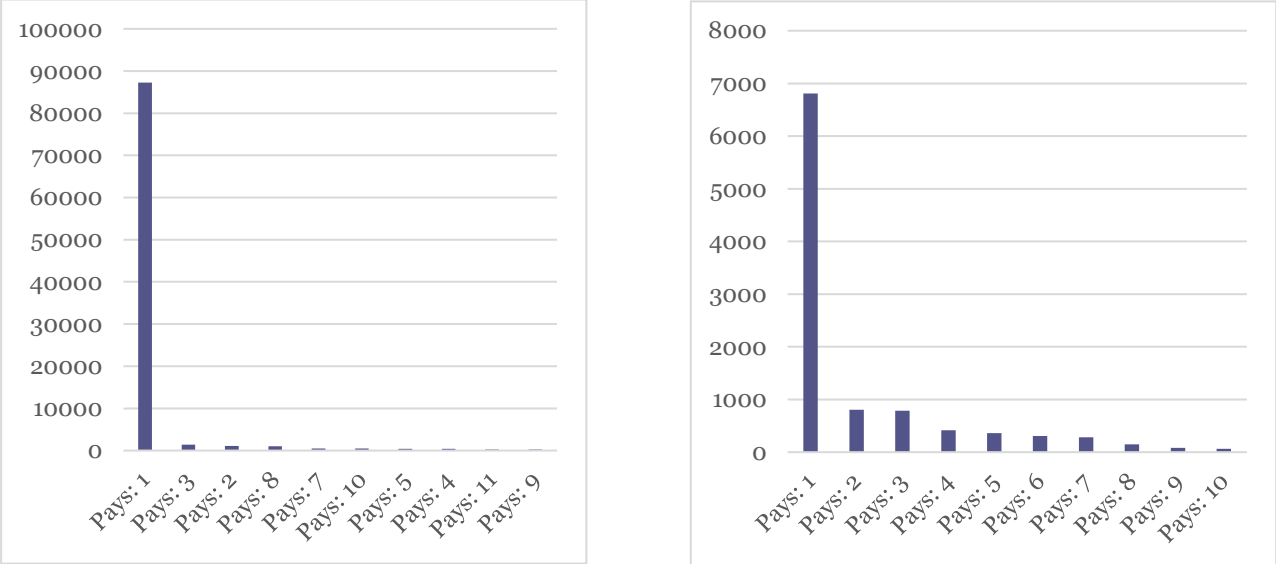


Figure 30 : Top 10 des 10 pays les plus représentés parmi les transactions frauduleuses (droite) et non frauduleuses (gauche) (Source : Interne)

Pour des raisons de confidentialité, les pays ont été anonymisés.

On observe que parmi les transactions non frauduleuses (figure de droite), la majorité des transactions sont effectuées en France, pour les transactions frauduleuses, la distribution est légèrement plus homogène et on constate que des transactions effectuées dans certains pays sont plus sujettes à la fraude.
Nous décidons de créer une variable nommée COUNTRY_RISQUE prenant la valeur 1 si le pays de la transaction est inclus dans les 10 pays ci-dessus et 0 autrement.

3.2.5) Distribution du nombre de transactions frauduleuses par type de transaction

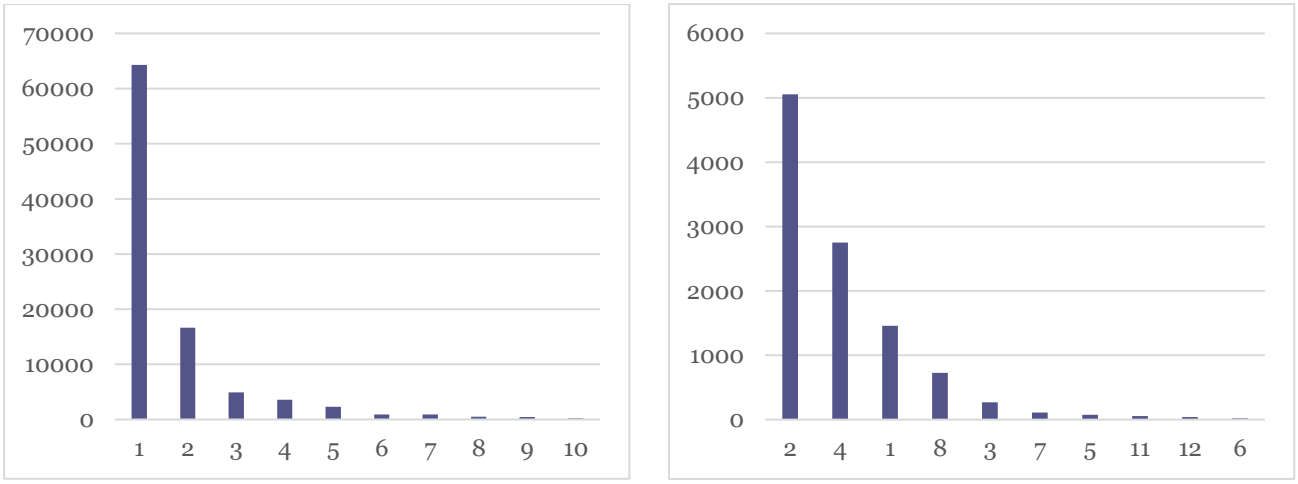


Figure 31 : Top 10 des codes transactions les plus représentés parmi les transactions frauduleuses (droite) et non frauduleuses (gauche) (Source : Interne)

Pour des raisons de confidentialité, les types de transactions ont été anonymisés.

De la même manière, lorsque l'on observe ces histogrammes il nous apparait ce ne sont pas les mêmes transactions qui sont les plus représentées entre les transactions frauduleuses et légitimes.

Nous décidons de nouveau de créer une variable FTTC_RISQUE en prenant cette fois-ci uniquement les 4 types de transactions les plus représentés parmi les transactions frauduleuses (figure de gauche).

3.2.6) Distribution du nombre de transactions frauduleuses par type de code marchand

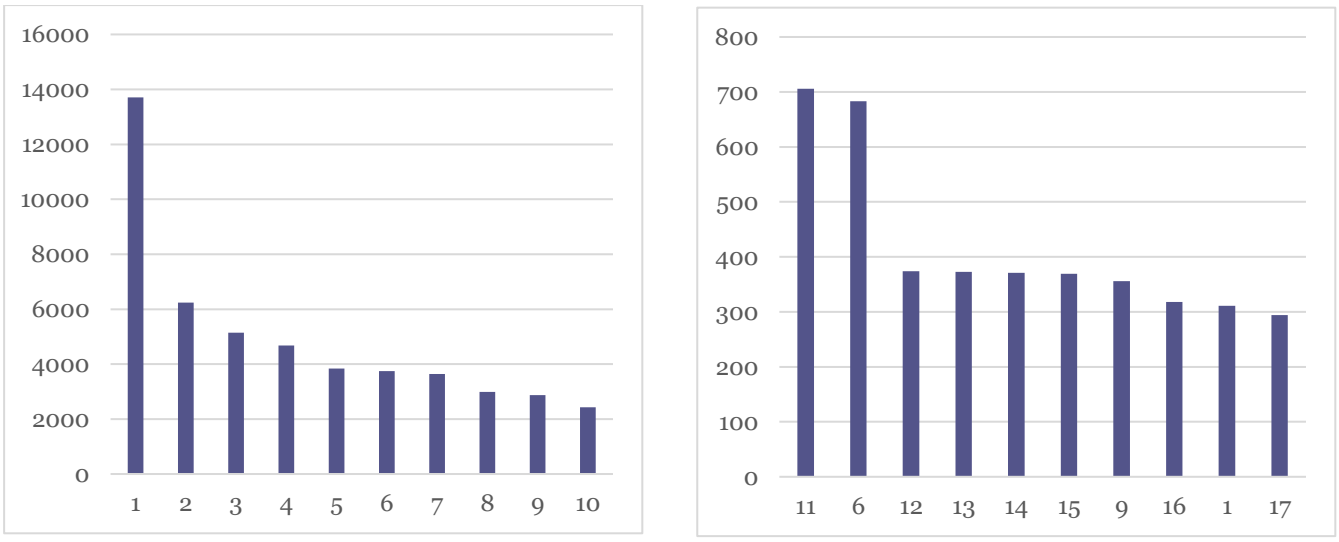


Figure 32 : Top 10 des codes marchands les plus représentés parmi les transactions frauduleuses et non frauduleuses (Source : Interne)

Pour des raisons de confidentialité, les types de marchands ont été anonymisés.

Ici encore, le type de code marchand diffère entre les transactions frauduleuses (figure de gauche) et les transactions légitimes (figure de droite). Nous créons de nouveau une variable MCC_RISQUE avec les 10 valeurs les plus représentées.

3.3) Analyse par corrélation

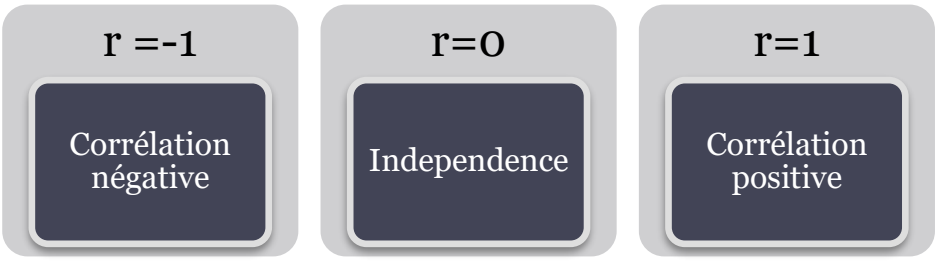
Une fois l'étude visuelle effectuée, nous décidons d'approcher le problème de la sélection de variables par des méthodes statistiques, ici, la corrélation de Pearson.
La réduction de variables permet, d'une part, de réduire la puissance de calcul nécessaire pour faire fonctionner notre modèle, et d'autre part, elle permet de le rendre plus robuste aux nouvelles données.

Plus le modèle est simple, plus il est facile de l'estimer, mais moins il est proche de la réalité.
Plus le modèle est complexe, plus il s'approche de la réalité, mais plus on risque de se tromper en l'estimant.
Dilemme complexité/performance : il faut trouver la complexité optimale.

La corrélation de Pearson ne fonctionnant que sur des données numériques nous dichotomisons les variables catégorielles par l'algorithme one hot encoder.
Pour rappel le coefficient de corrélation de Pearson noté r se calcule ainsi :

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}}$$

Il s'interprète ainsi :



Nous analysons le r de Pearson entre la variable cible et les variables explicatives, et on ne sélectionne que les variables ayant une valeur absolue supérieure à 0.09 avec la variable cible.

Nous obtenons ainsi :

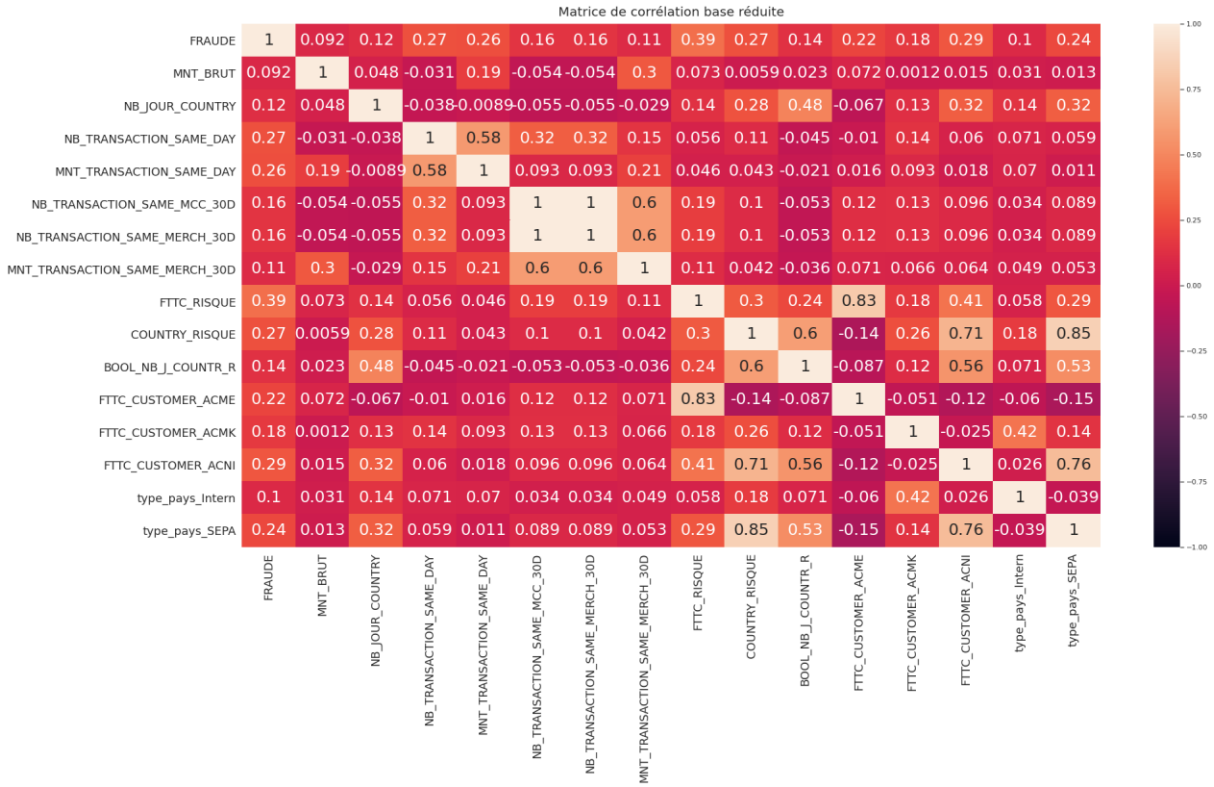


Figure 33 : Matrice de corrélation afin d'analyser la multi colinéarité (Source : Interne)

On constate à travers cette matrice de corrélation que plusieurs variables explicatives sont corrélées entre elles. La multi colinéarité n'influe pas sur la performance de la prédiction, mais elle rend difficile la compréhension du modèle nous allons donc supprimer certaines variables transportant à priori la même information.

Nous conserverons ces variables pour notre modèle :

Variable conservée pour modèle
FRAUDE
NB_TRANSACTION_SAME_DAY
NB_TRANSACTION_SAME_MERCH_30D
FTTC_RISQUE
COUNTRY_RISQUE
type_pays_Intern
type_pays_SEPA
NB_JOUR_COUNTRY

3.4) Découpage de la base en échantillons d'apprentissage et de test

Pour les besoins du modèle, nous allons découper notre population en 2 échantillons, un échantillon d'apprentissage sur lequel nous allons faire « apprendre » notre modèle et un échantillon de test sur lequel nous allons tester le modèle construit précédemment.

Cette étape permet d'identifier un potentiel sur apprentissage (phénomène qui arrive lorsque notre modèle « apprend » trop sur les données et n'est pas capable de fonctionner de manière optimale sur de nouvelles données).

3.4.1) Validation croisée et optimisation des hyperparamètres

Lorsque nous découpons notre base d'étude en échantillons d'apprentissage et de test nous n'avons qu'un seul échantillon pour affûter notre modèle et un seul pour le tester.

Une technique consiste à découper notre base d'apprentissage en plusieurs parties, par exemple, 5.

Tour à tour, chaque partie deviendra l'échantillon de test et les autres parties l'échantillon d'apprentissage.
Durant cette étape, nous pouvons optimiser les hyperparamètres de notre modèle en testant plusieurs valeurs pour chaque itération.

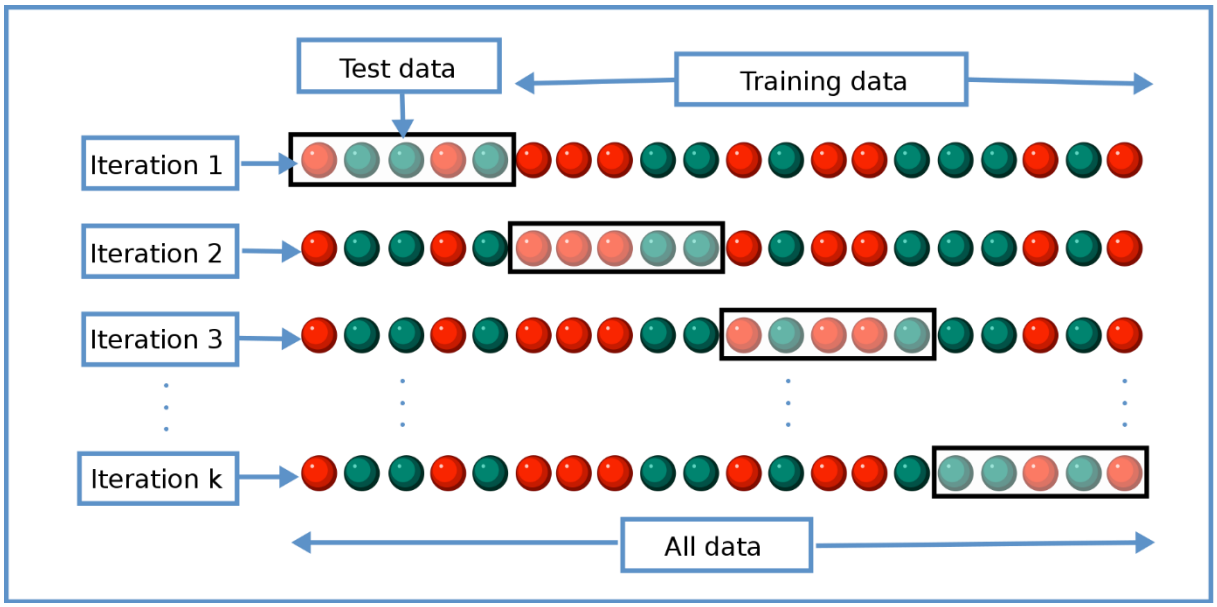


Figure 34 : Exemple de validation croisée (Source : https://towardsdatascience.com/cross-validation-c4fae714f1c5)

3.5) Régression logistique

La régression logistique vise à construire un modèle permettant d'expliquer les valeurs prises par une variable cible catégorielle à partir d'un ensemble de variables explicatives qui peuvent être quantitatives ou qualitatives. La variable à expliquer est le plus souvent binaire, nous parlons alors de régression logistique binaire. Une régression logistique se définit par une équation de type :

$$Y = \beta_0(X_0) + \beta_1(X_1) + \cdots + \beta_n(X_n)$$

∗ avec X_i la variable explicative et β_i le coefficient appliqué à cette variable Vi

On lance donc une régression logistique avec les variables précédemment identifiées.

3.5.1) Performance du modèle

Afin d'évaluer la performance d'un modèle de classification plusieurs paramètres sont envisageables.

Beaucoup se basent sur la matrice de confusion qui identifie les faux positifs, vrais positifs, faux négatifs et vrais positifs.

	Réel : Transaction frauduleuse	**Réel : Transaction non frauduleuse**
Prédiction : Transaction frauduleuse	Vrai positif (VP)	Faux positif (FP)
Prédiction : Transaction non frauduleuse	Faux négatif (FN)	Vrai négatif (VN)

Dont :

- L'exactitude (Accuracy en anglais) qui permet de calculer sur toutes les prédictions le nombre de prédictions correctes
  - Exactitude = VP+VN/Total
- La précision qui permet d'évaluer la qualité de la prédiction uniquement sur l'évènement « 1 »
  - Précision = VP/VP+FP
- Sensibilité évalue la probabilité que la prédiction soit égale à 1 parmi les évènements égaux à 1
  - VP/VP+FN
- Spécificité évalue la probabilité que la prédiction soit égale à 0 parmi les évènements égaux à 0
  - VN/VN+FP

Quand la variable étudiée est distribuée hétérogènement (c'est le cas ici avec 10 % de fraudeur), l'Accuracy n'est pas la meilleure métrique, car elle sera biaisée par le nombre de vrais négatifs. Comme ils seront très nombreux la capacité à les identifier sera forte.

Un Score appelé le F1 Score permet d'évaluer la fiabilité d'un modèle avec une distribution hétérogène de la variable cible. C'est celui-ci que nous utiliserons pour optimiser nos paramètres et évaluer notre modèle. Le F1 score regroupe la précision et la spécificité dans une seule métrique.

$$F1\ Score = 2 * \frac{Précision * Spécificité}{Précision + Spécificité}$$

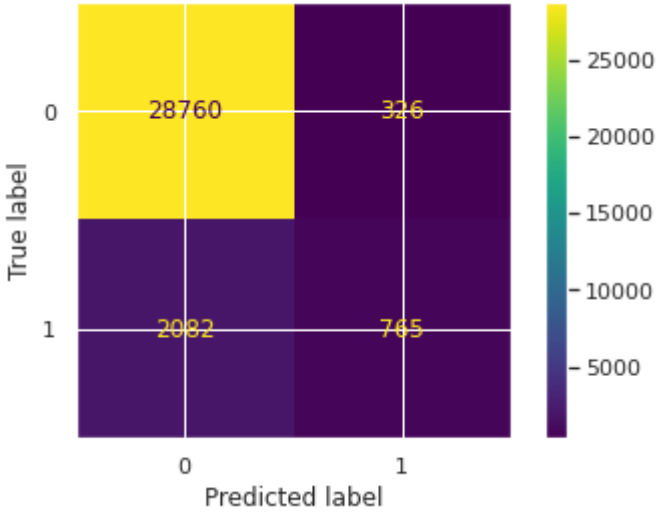


Figure 35 : Matrice de confusion de la régression logistique (Source : Interne)

Comme expliqué plus haut, ici, le taux de vrais négatifs est extrêmement élevé, on obtient donc une Accuracy élevée, mais la métrique n'est pas fiable.

- Accuracy = VP+VN/Total
  - Accuracy= 765+28760/31933
  - Accuracy= 0.9245
- Précision = VP/VP+FP
  - Précision = 765/765+326
  - Précision = 0,7011
- Spécificité = VN/VN+FP
  - Spécificité = 28760/28760+326
  - Spécificité =0.9887
- F1 Score = $2 * \frac{Précision * Spécificité}{Précision + Spécificité}$
  - F1 Score = $2 * \frac{0.7011 * 0.9887}{0.7011 + 0.9887}$
  - F1 Score =0.92

On peut aussi calculer le F1 Score pour la classe à trouver ici, F1 Score vaut 0.39 pour l'événement « 1 »

3.6) Forêt Aléatoire

Nous allons créer un nouveau modèle basé sur une forêt aléatoire.

Comme évoqué dans la partie dédiée, une foret aléatoire est un ensemble d'arbre de décisions, les arbres de décisions sont très populaires dans le domaine de la statistique et de la data-science, car ils sont flexibles, permettent d'utiliser plusieurs types de variables explicatives et à expliquer (arbre de classification ou de régression). Cependant, les arbres de décisions sont assez instables et une des solutions est de prendre la moyenne de plusieurs arbres de décisions.

On utilise, de la même manière que pour la régression, une validation croisée, on va tester notre modèle sur plusieurs échantillons avec plusieurs paramètres différents pour la forêt aléatoire (notamment la profondeur maximale du nœud et le nombre d'enregistrements minimum nécessaire pour couper un nœud interne).

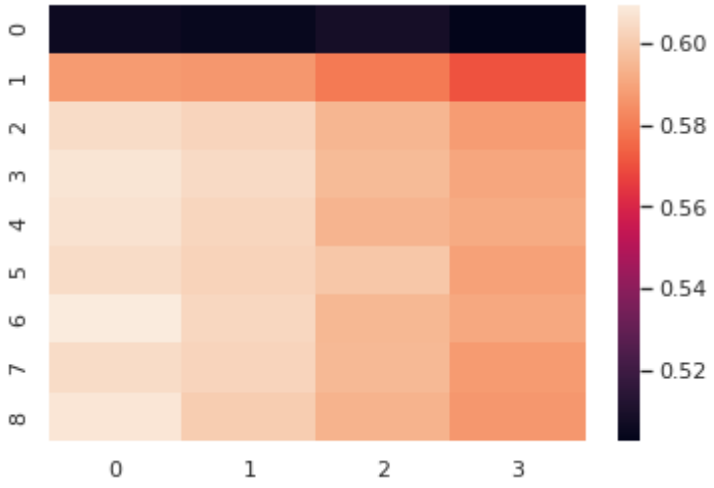


Figure 36: Heatmap des meilleurs résultats avec plusieurs paramètres testés (Source : Interne)

Une fois les meilleurs paramètres obtenus avec une forêt aléatoire à 100 arbres on relance notre modèle avec les paramètres optimaux cette fois-ci, mais sur 10000 arbres.

On obtient cette matrice de confusion :

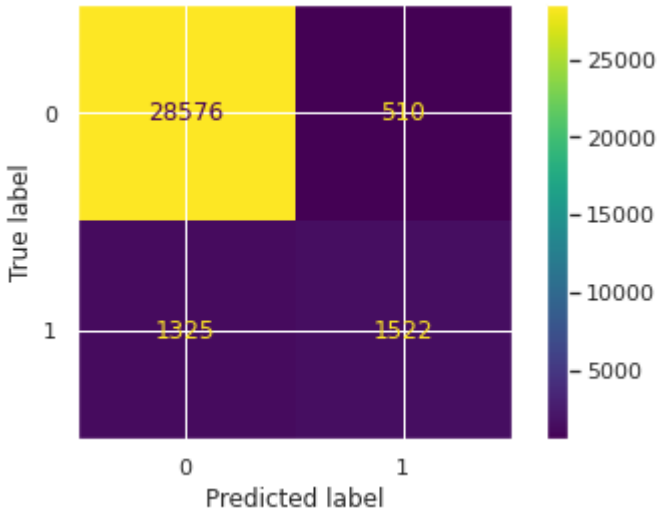


Figure 37 : Matrice de confusion de la random Forest (Source : Interne)

Avec un F1 Score égal à 0.63 pour la classe 1 et une Accuracy égale à 0.94

La random Forest permet d'obtenir de meilleurs résultats, mais elles sont aussi plus coûteuses en ressource et en configuration.
Les résultats obtenus au vu des moyens mis à disposition sont corrects, il conviendrait d'optimiser plus de paramètres ainsi que d'obtenir par exemple les heures et minutes des transactions au vu de l'importance des variables contenant l'information sur les fréquences de transactions.

4) Conclusion

La carte bancaire est la face émergée de l'iceberg, cette carte de paiement en plastique dont l'utilisation est très simple cache un système monétique extrêmement complexe et codifié. Comme les autres moyens de paiements (chèques, virement), la carte bancaire est un moyen de paiement victime de nombreuses fraudes.

L'analyse des différents types de fraudes nous a permis de comprendre que les fraudeurs pouvaient être très ingénieux dans l'élaboration des techniques déjouant les derniers systèmes de sécurité.
Ils profitent toujours des dernières nouveautés par les systèmes de paiement afin de trouver de nouveaux moyens de frauder (on pense notamment au paiement sans contact).
Aujourd'hui, les moyens de paiements évoluent très rapidement ; en quelques années, nous avons vu apparaitre le paiement sans contact, le paiement par mobile, et le paiement biométrique.
Toutes ces évolutions doivent être accompagnées à la fois par des moyens techniques, et par les institutions.

Les acteurs du système monétique eux aussi redoublent d'efforts et mettent au point des techniques toujours plus innovantes et performantes afin de lutter contre la fraude monétique, elles peuvent aujourd'hui se reposer sur une volumétrie et une qualité de la donnée grandissante, ces données permettent d'avoir une analyse plus fine des tenants et aboutissants autour de la fraude à la carte bancaire et de développer des modèles plus performants.

Cependant la technique à elle seule ne peut pas suffire, elle doit se faire sous l'impulsion des grandes institutions (État, Europe). L'initiative DSP2 a permis de réduire de manière considérable la fraude monétique. La collaboration entre les pays et l'utilisation des leviers que peut offrir l'Union européenne sont essentielles.

Glossaire

ML : Machine Learning

ATM : Automatic Teller Machine

BCE : Banque centrale européenne

CB : Carte bancaire

NFC : Near Filed Communication

OSCM : Observatoire de sécurité des moyens de paiements

POS : Point Of Sale

TPE : Terminal de Paiement électronique

Bibliographie

[1] Éric Benhamou,« Seize banques européennes s'unissent pour s'affranchir de Visa et Mastercard | Les Echos ». https://www.lesechos.fr/finance-marches/banque-assurances/seize-banques-europeennes-sunissent-pour-saffranchir-de-visa-et-mastercard-1220762

[2] G. Ataya, « PCI DSS audit and compliance », *Information Security Technical Report*, vol. 15, nº 4, p. 138-144, nov. 2010, doi: 10.1016/j.istr.2011.02.004.

[3] M. J. Stephey, « A Brief History of: Credit Cards », *TIME Magazine*, vol. 173, nº 17, p. 16-16, mai 2009.

[4] P. Trescases, « Cartes bancaires et technologies : le système CB », *Les Cahiers du numerique*, vol. Vol. 4, nº 1, p. 177-184, 2003.

[5] N. E. Madhoun et G. Pujolle, « Security Enhancements in EMV Protocol for NFC Mobile Payment », in *2016 IEEE Trustcom/BigDataSE/ISPA*, août 2016, p. 1889-1895. doi: 10.1109/TrustCom.2016.0289.

[6] Alex Rolfe, « US market hits 1 billion EMV chip cards milestone behind Asia », *Payments Cards & Mobile*, juin 01, 2020. https://www.paymentscardsandmobile.com/us-market-hits-1-billion-emv-chip-cards-milestone/.

[7] Norme ISO, « ISO/IEC 7811-2:2014 », *ISO*. https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/06/19/61936.html.

[8] Norme ISO, « ISO/IEC 7811-4:1995 », *ISO*. https://www.iso.org/cms/render/live/fr/sites/isoorg/contents/data/standard/01/47/14723.html.

[9] S. J. Murdoch, S. Drimer, R. Anderson, et M. Bond, « Chip and PIN is Broken », in *2010 IEEE Symposium on Security and Privacy*, mai 2010, p. 433-446. doi: 10.1109/SP.2010.33.

[10] B. Al Smadi et M. Min, « A Critical review of Credit Card Fraud Detection Techniques », in *2020 11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, oct. 2020, p. 0732-0736. doi: 10.1109/UEMCON51285.2020.9298075.

[11] S. Hamdare, V. Nagpurkar, et J. Mittal, « Securing SMS Based One Time Password Technique from Man in the Middle Attack », *IJETT*, vol. 11, nº 3, p. 154-158, mai 2014, doi: 10.14445/22315381/IJETT-V11P230.

[12] E. C. Bank, « Card payments in Europe – current landscape and future prospects: a Eurosystem perspective », *European Central Bank*, avr. 17, 2019. https://www.ecb.europa.eu/pub/pubbydate/2019/html/ecb.cardpaymentsineu_currentlandscapeandfutureprospects201904~30d4de2fc4.en.html.

[13] « Rapports d'activité », *Banque de France*, mai 12, 2017. https://www.banque-france.fr/liste-chronologique/rapports-dactivite (consulté le août 30, 2021).

[14] « Missions », *Banque de France*, mai 12, 2017. https://www.banque-france.fr/stabilite-financiere/observatoire-de-la-securite-des-moyens-de-paiement/missions.

[15] J. Devèze, A. Couret, I. Parachkévova-Racine, T. Poulain-Rehm, M.Teller, V. Mauriès, « Directives européennes et transposition en droit national ». Wolters Kluwer France, juin 27, 2016. [En ligne]. Disponible sur: https://www-lamyline-fr.proxybib-pp.cnam.fr/content/document.aspx?idd=DT0001754261&version=vigente&DATA=8DEi7eei490SFO33e809ycYF044eriu8

[16] A. Teixeira, « Analyse discrimante par arbre de décision binaire (CART : Classification And Regression Tree) », *Revue des Maladies Respiratoires*, vol. 21, nº 6, p. 1174-1176, déc. 2004, doi: 10.1016/S0761-8425(04)71596-X.

[17] Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, J. Christopher Westland « Data mining for credit card fraud: A comparative study - ScienceDirect ». https://www-sciencedirect-com.proxybib-pp.cnam.fr/science/article/pii/S0167923610001326?via%3Dihub

Code permettant d'optimiser les paramètres de la random forest :

```
from sklearn.model_selection import cross_val_score
# Liste.
depth_values = range(10, 100, 10)
min_samples_split_values = range(2, 10, 2)

#
print(X.shape)
model = RandomForestClassifier(n_estimators = 100, n_jobs = -1)

scores = list()

for depth in depth_values:
    model.max_depth = depth
    list_tmp = list()
    list_tmp_2 = list()
    for min_samples_split in min_samples_split_values:
        model.min_samples_split = min_samples_split
        this_scores = cross_val_score(model, X_train, y_train,
                                      cv=5, n_jobs=-1,scoring='f1')
        list_tmp.append(np.mean(this_scores))
    scores.append(list_tmp)
```

Code de transaction FTTC_CUSTOMER :

TRANSACTION_TYPE	DESCRIPTION
ACM0	RETRAIT DAB FRANCE
ACM4	RETRAIT DAB HZ.EUR-DT CPT CLT
ACMC	PAIEMENT CB FRANCE - PROXIMITE
ACME	PAIEMENT CB FRANCE - WEB
ACMG	PAIEMENT CB HZ.EUR-DT CLT-PROX
ACMK	PAIEMENT CB HZ.EUR-DT CLT-WEB
ACMO	AVOIR CB FRANCE - PROXIMITE
ACMQ	AVOIR CB FRANCE - WEB
ACMS	AVOIR CB HZ.EUR-CT CLT-PROX
ACMW	AVOIR CB HZ.EUR-CT CLT-WEB
ACN6	RETRAIT DAB Z.EUR-DT CPT CLT
ACNE	PAIEMENT CB Z.EUR-DT CLT-PROX
ACNI	PAIEMENT CB Z.EUR-DT CLT-WEB
ACNQ	AVOIR CB Z.EUR-CT CLT-WEB

Référence code mcc :

MCC_CODE	DESCRIPTION
0742	Veterinary Services
0763	Agricultural Cooperatives
0780	Landscaping and Horticultural Services
1520	General Contractor/Residential Building
1711	Heating, Plumbing, Air Conditioning Contractors
1731	Electrical Contractors
1740	Masonry, Stonework, Tile Setting, Plastering, Insulation Contractors
1750	Carpentry
1761	Roof, Siding, and Sheet Metal Work Contractors
1771	Contractors, Concrete
1799	Special Trade Contractor - Not Elsewhere Classified
2741	Miscellaneous Publishing and Printing Services
2791	Typesetting, Plate Making and Related Services (Business to Business MCC)
2842	Specialty Cleaning, Polishing and Sanitation Preparations (Business to Business MCC)
3000	United Airlines
3001	American Airlines
3005	British Airways
3006	Japan Air Lines
3007	Air France
3008	Lufthansa
3009	Air Canada
3010	KLM
3011	AeroFlot
3012	Qantas
3013	Alitalia
3015	SWISS
3016	SAS
3017	South African Airway
3018	Varig (Brazil)
3020	Air India
3021	Air Algerie
3025	Air New Zealand Ltd.
3026	Emirates Airlines
3028	Air Malta
3029	SN Brussels Airlines - SN BRUSSELS
3030	Aerolineas Argentinas
3032	El Al
3034	ETIHADAIR
3035	TAP (Portugal)
3037	EgyptAir
3039	Avianca
3042	FinnAir
3043	Aer Lingus

3047	THY (Turkey)
3048	Royal Air Maroc
3049	Tunis Air
3050	Icelandair
3051	Austrian Airlines
3052	LANAIR
3056	JetAir
3058	Delta
3064	Adria Airways
3066	Southwest
3068	AIR STANA
3072	CEBU PAC
3075	Singapore Airlines
3076	Aeromexico
3077	Thai Airways
3078	China Airlines
3079	Jetstar Airways - Jetstar
3082	Korean Airlines
3084	Eva Airlines
3098	Asiana Airlines
3099	Cathay Pacific
3100	Malaysian Airline Sys
3102	Iberia
3127	Taca International
3136	Qatar Air
3146	Luxair
3161	All Nippon Airways
3174	JetBlue Airways
3175	Middle East Air
3180	Westjet Airlines-WESTJET
3182	LOT (Poland)
3183	Oman Aviation - OMAN AIR
3206	China Eastern Airlines (Abbr: China East Air)
3211	Norwegian Air Shuttle - NORWEGIANAIR
3217	CSA-Ceskoslovenske Aeroln
3220	Compania Faucett
3223	Comair
3234	CARIBAIR
3236	Air Arabia Airlines - Air Arab
3240	Bahamasair
3245	Easy Jet - EASYJET
3246	Ryan Air - RYANAIR
3247	Gol Airlines - GOL
3248	Tam Airlines - TAM

3256	Alaska Airlines Inc.
3260	Spirit Airlines - SPIRIT
3261	Air China
3266	Air Seychelles
3294	Ethiopian Airlines
3295	Kenya Airways
3296	Air Berlin-AIRBERLIN
3297	Tarom Romanian Air Transport
3298	Air Mauritius
3351	Affiliated Auto Rental
3355	SIXT Car Rental
3357	Hertz
3364	Agency Rent a Car
3366	Budget Rent a Car
3374	Accent Rent-A-Car
3381	Europ Car
3387	Alamo Rent a Car
3389	Avis R-A-C
3390	Dollar R-A-C
3393	National Car Rental
3395	Thrify Car Rental
3405	Enterprise R-A-C
3409	General Rent-a-Car
3441	Advantage Rent A Car
3501	Holiday Inns
3502	Best Western Hotels
3503	Sheraton
3504	Hilton
3506	Golden Tulip Hotels
3508	Quality Inns
3509	Marriott
3510	Days Inn Colonial Resort
3512	Intercontinental Hotels
3515	Rodeway Inn
3516	LaQuinta Motor Inns
3519	Pullman International Hotels
3520	Meridien Hotels
3530	Renaissance Hotels
3533	Hotel Ibis
3535	Hilton International
3537	ANA Hotels
3538	Concorde Hotels
3540	Iberotel Hotels
3542	Royal Hotels

3543	Four Seasons
3545	Shangri-La International
3548	Hotels Melia
3549	Auberge des Governeurs
3552	Coast Hotel
3553	Park Inn by Radisson
3555	Treasure Island Hotel and Casino
3559	Candlewood Suites
3562	Comfort Inns
3577	Mandarin Oriental Hotel
3579	Hotel Mercure
3583	Radisson BLU
3590	Fairmont Hotel
3592	Omni Hotels
3604	Hilton Garden Inn
3612	Movenpick Hotels
3615	Travelodge Motels
3617	America's Best Value Inn
3619	Aloft
3621	Extended Stay
3625	Hotel Universale
3633	Rank Hotels
3634	Swissotel
3635	Reso Hotel
3637	Ramada Inns
3638	Howard Johnson
3640	Hyatt Motels
3641	Sofitel Hotels
3642	Novotel
3644	EconoLodges
3649	Radisson
3653	Penta Hotels
3654	Loews Hotels
3655	Scandic Hotels
3657	Oberoi Hotels
3661	Metropole Hotels
3662	Circus Hotel and Casino
3665	Hampton Inn Hotels
3667	Luxor Hotel and Casino
3668	Maritim Hotels
3672	Campanile Hotels
3675	Interhotel CEDOK
3676	Monte Carlo Hotel and Casino
3677	Climat de France Hotels

3678	Cumulus Hotels
3681	Adams Mark Hotels
3687	Clarion Hotels
3690	Courtyard Inns
3692	Doubletree
3698	Harley Hotels
3700	Motel 6
3708	Virgin River Hotel and Casino
3709	Super 8 Motels
3715	Fairfield Inn
3716	Carlton Hotels
3719	Protea Hotels
3722	Wyndham Hotels
3726	Rio Suites
3730	MGM Grand Hotel
3740	Towneplace Suites
3741	Millennium Hotel
3750	Crown Plaza Hotels
3751	Homewood Suites
3765	Bellagio
3773	The Venetian Resort Hotel and Casino
3777	Mandalay Bay Resort
3778	Four Points Hotels
3780	Disney Resorts
3783	Town and Country Resort and Convention Center
3791	Staybridge Suites
3793	The Flamingo Hotels
3795	Paris Las Vegas Hotel
3811	Premier Travel Inn
3812	Hyatt Place
3813	Hotel Indigo
3825	Vdara
3828	Cosmopolitan of Las Vegas
3830	Park Plaza Hotel
3831	Waldorf
4011	Railroads
4111	Local and Suburban Commuter Passenger Transportation, including Ferries
4112	Passenger Rail (train)
4119	Ambulance Services
4121	Taxicabs and Limousines
4131	Bus Lines, includes Charters/Tour Buses
4214	Motor Freight Carriers and Trucking-Local and Long Distance, Moving & Storage Companies, and Local Delivery
4215	Courier Services-Air and Ground, and Freight Forwarders

4225	Public Warehousing-Farm products, Refrigerated Goods, Household Goods, and Storage
4411	Steamship and Cruise Lines
4457	Boat Rentals and Leasing
4468	Marinas, Marine Service, and Supplies
4511	Airlines and Air Carriers
4582	Airports, Flying Fields, and Airport Terminals
4722	Travel Agencies
4784	Bridge and Road Fees, Tolls
4789	Transportation Services-not elsewhere classified
4812	Telecommunication Equipment and Telephone Sales
4814	Telecommunication Services, Including Local and Long Distance Calls, Credit Card Calls, Call Through Use of Magnetic-Strip-Reading Telephones, and Fax Services
4816	Computer Network/Information Services and other Online Services such as electronic bulletin board, e-mail, web site hosting services, or Internet access
4829	Quasi Cash - Money Transfer
4899	Cable, Satellite, and Other Pay Television and Radio Services
4900	Utilities-Electric, Gas, Water, and Sanitary
5013	Motor Vehicle Supplies and New Parts (Business to Business MCC)
5021	Office Furniture (Business to Business MCC)
5039	Construction Materials Not Elsewhere Classified (Business to Business MCC)
5044	Photographic, Photocopy, Microfilm Equipment and Supplies (Business to Business MCC)
5045	Computers, Computer Peripheral Equipment, and Software
5046	Commercial Equipment Not Elsewhere Classified (Business to Business MCC)
5047	Dental/Laboratory/Medical/Ophthalmic Hospital Equipment and Supplies
5051	Metal Service Centers and Offices (Business to Business MCC)
5065	Electrical Parts and Equipment (Business to Business MCC)
5072	Hardware, Plumbing, Heat Equipment and Supplies (Business to Business MCC)
5074	Plumbing and Heating Equipment and Supplies (Business to Business MCC)
5085	Industrial Supplies Not Elsewhere Classified (Business to Business MCC)
5094	Precious Stones, Metals, Watches and Jewelry (Business to Business MCC)
5099	Durable Goods Not Elsewhere Classified (Business to Business MCC)
5111	Stationery, Office Supplies, and Printing and Writing Paper
5122	Drugs, Drug Proprietary's, and Druggists' Sundries
5131	Piece Goods, Notions and Other Dry Goods (Business to Business MCC)
5137	Men's, Women's and Children's Uniforms (Business to Business MCC)
5139	Commercial Footwear (Business to Business MCC)
5169	Chemicals and Allied Products Not Elsewhere Classified (Business to Business MCC)
5172	Petroleum and Products (Business to Business MCC)
5192	Books, Periodicals and Newspapers (Business to Business MCC)
5193	Florist Suppliers, Nursery Stock & Flowers (Business to Business MCC)
5198	Paints, Varnishes and Supplies (Business to Business MCC)
5199	Non-durable Goods Not Elsewhere Classified (Business to Business MCC)
5200	Home Supply Warehouse
5211	Lumber & Building Materials Stores

5231	Glass, Paint, and Wallpaper Stores
5251	Hardware Stores, Equipment Utilities Regulated
5261	Nurseries and Lawn and Garden Supply Stores
5271	Mobile Home Dealer
5300	Wholesale Club with or without membership fee
5309	Duty Free Stores
5310	Discount Store
5311	Department Stores
5331	Variety Stores
5399	Miscellaneous General Merchandise
5411	Grocery Stores and Supermarkets
5422	Freezer & Locker Meat Provisions
5441	Candy, Nut, and Confectionary Stores
5451	Dairy Product Stores
5462	Bakeries
5499	Miscellaneous Food Stores-Convenience Stores and Specialty Markets
5511	Car and Truck Dealers (New and Used)- Sales, Service, Repairs, Parts, and Leasing
5521	Car and Truck Dealers (Used)- Sales, Service, Repairs, Parts, and Leasing
5532	Automotive Tire Stores
5531	Auto and Home Supply Stores
5533	Automotive Parts and Accessories Stores
5541	Service Stations (with or without Ancillary Services)
5542	Automated Fuel Dispensers
5551	Boat Dealers
5561	Camper, Recreational and Utility Trailer Dealers
5571	Motorcycle Dealers
5592	Motor Home Dealers
5598	Snowmobile Dealers
5599	Miscellaneous Automotive, Aircraft, and Farm Equipment Dealers --Not Elsewhere Classified
5611	Men's & Boys' Clothing and Accessory Stores
5621	Women's Ready-to-Wear Stores
5631	Women's Accessory and Specialty Stores
5641	Children's and Infants' Wear Stores
5651	Family Clothing Stores
5655	Sports and Riding Apparel Stores
5661	Shoe Stores
5681	Furriers & Fur Shops
5691	Men's and Women's Clothing Stores
5697	Tailors, Seamstresses, Mending, Alterations
5698	Wig & Toupee Shops
5699	Miscellaneous Apparel and Accessory Stores
5712	Furniture, Home Furnishings, and Equipment Stores, except Appliances
5713	Floor coverings, Rugs
5714	Drapery, Window Covering, and Upholstery Stores

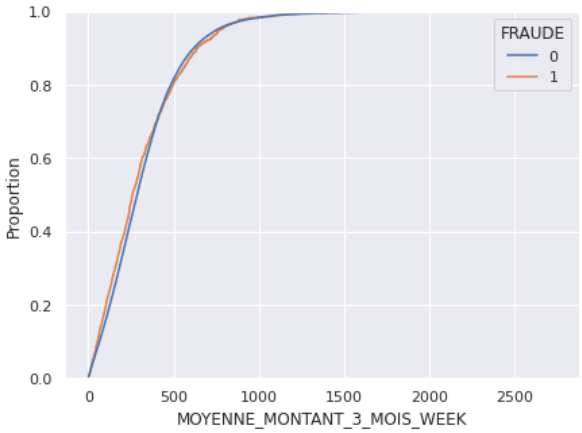
5719	Miscellaneous Home Furnishing Specialty Stores
5722	Household Appliance Stores
5732	Electronics Stores
5733	Music Stores-Musical Instruments, Pianos, and Sheet Music
5734	Computer Software Stores
5735	Record Stores
5811	Caterers - Prepare & Delivery
5812	Eating Places and Restaurants
5813	Drinking Places (Alcoholic Beverages) - Bars, Taverns, Nightclubs, Cocktail Lounges, and Discotheques
5814	Quick Payment Service-Fast Food Restaurants
5815	Digital Goods – Media, Books, Movies, Music
5816	Digital Goods – Games
5817	Digital Goods – Applications (Excludes Games)
5818	Large Digital Goods Merchant
5912	Drug Stores and Pharmacies
5921	Package Stores--Beer, Wine, and Liquor
5931	Used Merchandise and Secondhand Stores
5932	Antique Shop
5933	Pawn Shop
5935	Wrecking and Salvage Yards
5937	Antique Reproduction Stores
5940	Bicycle Shop-Sales and Services
5941	Sporting Goods Stores
5942	Book Stores
5943	Stationery, Office and School Supply Stores
5944	Jewelry, Watch, Clock, and Silverware Stores
5945	Hobby, Toy and Game Stores
5946	Camera and Photographic Supply Stores
5947	Gift, Card, Novelty, and Souvenir Stores
5948	Luggage and Leather Goods Stores
5949	Sewing, Needlework, Fabric, and Piece Good Stores
5950	Glassware and Crystal Stores
5960	Direct Marketing Insurance Services
5962	Direct Marketing -- Travel Related Arrangement Services
5963	Direct Selling Establishments/Door to Door Sales
5964	Catalog Merchant
5965	Combined Catalog and Retail Merchant
5966	Outbound Telemarketing Merchant
5967	Direct Marketing -- Inbound Telemarketing Merchants
5968	Continuity/Subscription Merchants
5969	Direct Marketing/Direct Marketers--Not Elsewhere Classified
5970	Artist Supply and Craft Stores
5971	Art Dealers and Galleries

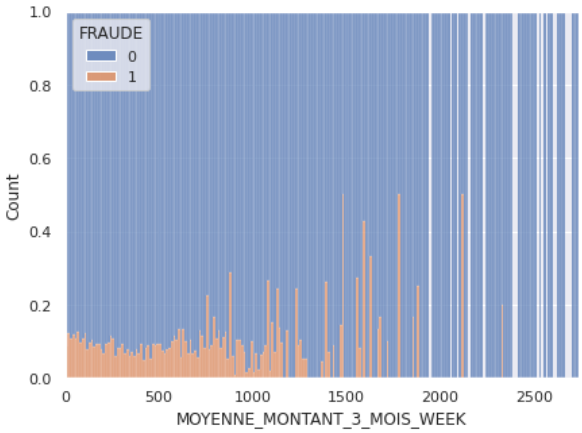
5972	Stamp and Coin Stores
5973	Religious Goods Stores
5975	Hearing Aids--Sales, Service, and Supplies
5976	Orthopedic Goods and Prosthetic Devices
5977	Cosmetic Stores
5983	Fuel Dealers--Fuel Oil, Wood, Coal, and Liquefied Petroleum
5992	Florists
5993	Cigar Stores & Stands
5994	News Dealers & Newsstands
5995	Pet Shops, Pet Food, and Supplies
5996	Swimming Pools--Sales, Supplies, and Services
5997	Electric Razor Stores Sales & Services
5998	Tent and Awning Stores
5999	Miscellaneous & Specialty Retail Stores
6010	Financial Institutions--Manual Cash Disbursements
6011	Financial Institutions--Automated Cash Disbursements
6012	Quasi Cash - Financial Institution - Merchandise and Services
6050	Quasi Cash - Member Financial Institution
6051	MasterCard - Quasi Cash-Merchant
	Visa - Non-Financial Institutions - Foreign Currency, Money Orders(not wire Transfer), & Travelers Cheques
6211	Securities - Brokers and Dealers
6300	Insurance Sales and Underwriting
6513	Real Estate Agents and Managers - Rentals; Property Management
6540	POI Funding Transactions (Excluding MoneySend)
7011	Lodging - Hotels, Motels, and Resorts
7012	Timeshares
7032	Sporting and Recreational Camps
7033	Trailer Parks and Campgrounds
7210	Laundry, Cleaning, and Garment Services
7211	Laundry Services - Family and Commercial
7216	Dry Cleaners
7221	Photographic Studios
7230	Beauty and Barber Shops
7251	Shoe Repair Shops, Shoe Shine Parlors, and Hat Cleaning Shops
7261	Funeral Services and Crematories
7273	Dating Services
7276	Tax Preparation Services
7277	Counseling Services - Debt, Marriage, and Personal
7278	Buying and Shopping Services and Clubs
7296	Clothing Rental - Costumes, Uniforms and Formal Wear
7297	Massage Parlors
7298	Health and Beauty Spas
7299	Miscellaneous Personal Services - Not Elsewhere Classified

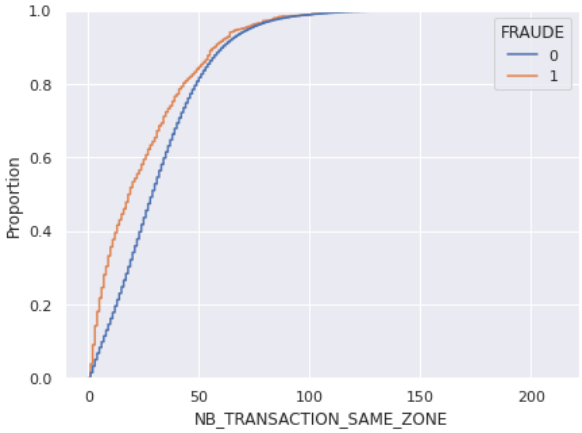
7311	Advertising Services
7321	Consumer Credit Reporting Agencies
7333	Commercial Photography, Art, and Graphics
7338	Quick Copy, Reproduction Service
7339	Stenographic Service
7349	Cleaning, Maintenance & Janitorial Services
7361	Employment Agencies and Temporary Help Services
7372	Computer Programming, Data Processing, and Integrated Systems Design Services
7375	Information Retrieval Services (Business to Business MCC)
7379	Computer Maintenance, Repair and Services (Business to Business MCC)
7392	Management, Consulting, and Public Relations Services
7393	Detective Agencies, Protective Agencies, and Security Services, including Armored Cars and Guard Dogs
7394	Equipment, Tool, Furniture, and Appliance Rental and Leasing
7395	Photofinishing Laboratories and Photo Developing
7399	Business Services
7512	Automobile Rental Agency
7513	Truck and Utility Trailer Rentals
7519	Motor Home and Recreational Vehicle Rentals
7523	Parking Lots and Garages
7534	Tire Retreading & Repair
7538	Automotive Service Shops (Non-Dealer)
7542	Car Washes
7549	Towing Services
7622	Electronic Repair Shops
7623	Air Conditioning and Refrigeration Repair Shops
7629	Electrical and Small Appliance Repair Shops
7631	Watch, Clock, and Jewelry Repair Shops
7641	Furniture - Reupholster, Repair, and Refinishing
7692	Welding Services
7699	Miscellaneous Repair Shops and Related Services
7829	Motion Picture & Video Tape Production and Distribution (Business to Business MCC)
7832	Motion Picture Theater
7841	DVD/Video Tape Rental Stores
7911	Dance Halls, Studios & Schools
7922	Theatrical Producers (except Motion Pictures) and Ticket Agencies
7929	Bands, Orchestras & Misc Entertainment
7932	Billiards & Pool Establishments
7941	Commercial Sports, Professional Sports Clubs, Athletic Fields, and Sports Promoters
7991	Tourist Attractions and Exhibits
7992	Public Golf Courses
7993	Video Amusement Game Supply
7994	Video Game Arcades and Establishments

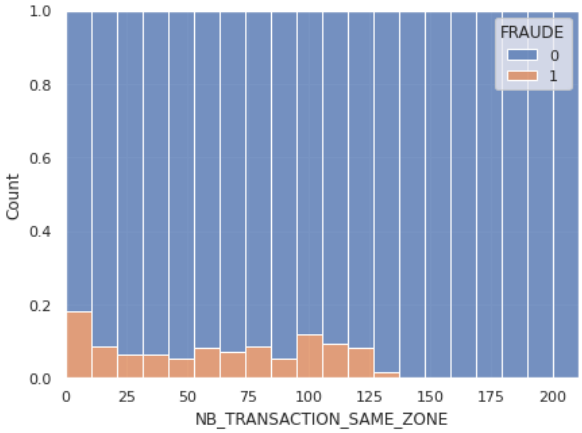
7995	Betting, including Lottery Tickets, Casino Gaming Chips, Off- Track Betting, and Wagers at Race Track
7996	Amusement Parks, Circuses, Carnivals, and Fortune Tellers
7997	Membership Clubs (Sports, Recreation, Athletic), Country Clubs, and Private Golf Courses
7998	Aquarium, Seaquarium, Dolphinariums
7999	Recreation Services - Not Elsewhere Classified
8011	Doctors and Physicians - Not Elsewhere Classified
8021	Dentists and Orthodontists
8041	Chiropractors
8042	Optometrists and Ophthalmologists
8043	Opticians, Optical Goods and Eyeglasses
8050	Nursing and Personal Care Facilities
8062	Hospitals
8071	Medical and Dental Laboratories
8099	Medical Services Health Practitioners - No Elsewhere Classified
8111	Legal Services and Attorneys
8211	Elementary and Secondary Schools
8220	Colleges, Universities, Professional Schools, and Junior Colleges
8241	Correspondence Schools
8244	Business and Secretarial Schools
8249	Trade and Vocational Schools
8299	Schools and Educational Services - Not Elsewhere Classified
8351	Child Care Services
8398	Charitable and Social Service Organizations
8641	Civic, Social, and Fraternal Associations
8651	Political Organizations
8661	Religious Organizations
8675	Automobile Associations
8699	Membership Organizations - Not Elsewhere Classified
8734	Testing Laboratories (Not Medical) - (Business to Business MCC)
8911	Architectural, Engineering, and Surveying Services
8931	Accounting, Auditing, and Bookkeeping Services
8999	Professional Services - Not Elsewhere Classified
9211	Court Costs, including Alimony and Child Support
9222	Fines
9311	Tax Payments
9399	Government Services - Not Elsewhere Classified
9402	Postal Services
9405	U.S. Fed Government Agencies

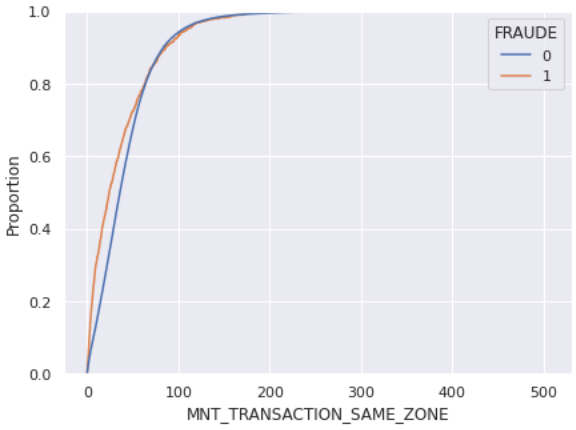
Autres graphiques :

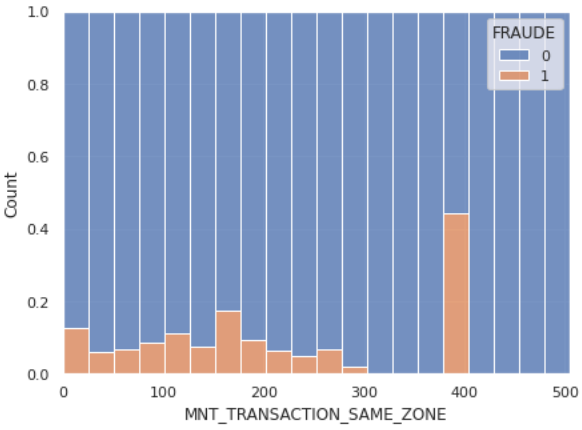

FRAUDE
0
1
Proportion
MOYENNE_MONTANT_3_MOIS_WEEK

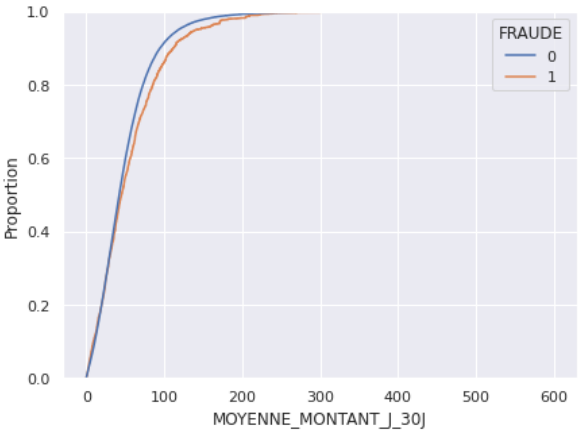

FRAUDE
0
1
Count
MOYENNE_MONTANT_3_MOIS_WEEK

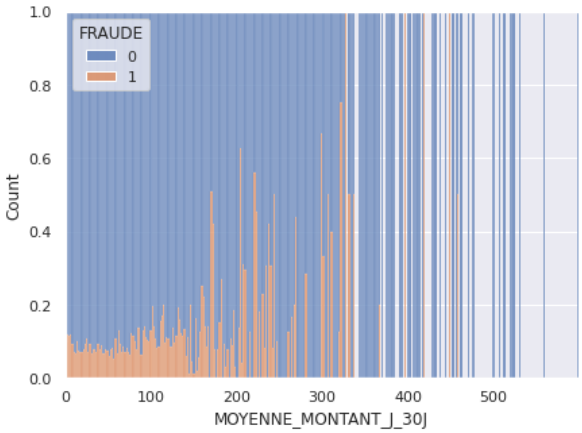

FRAUDE
0
1
Proportion
NB_TRANSACTION_SAME_ZONE

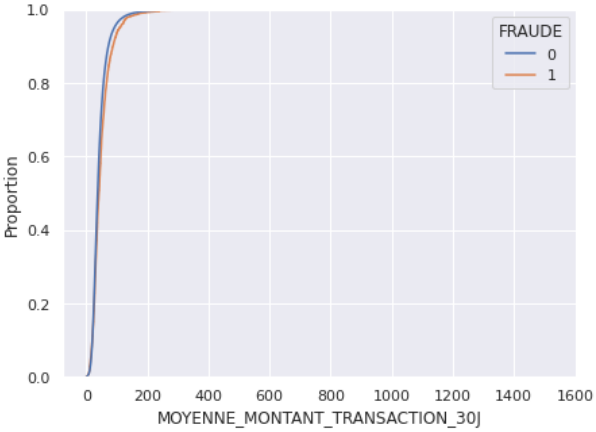

FRAUDE
0
1
Count
NB_TRANSACTION_SAME_ZONE

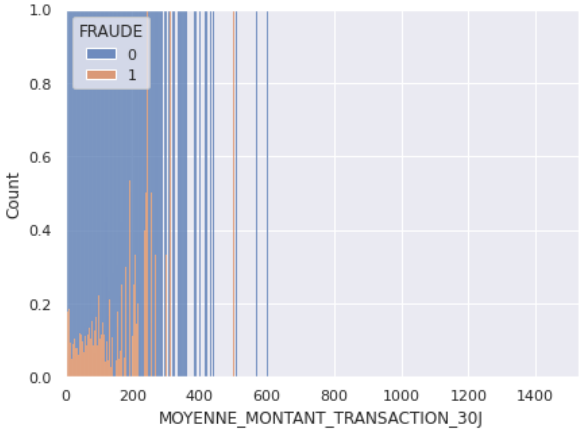

FRAUDE
0
1
Proportion
MNT_TRANSACTION_SAME_ZONE


FRAUDE
0
1
Count
MNT_TRANSACTION_SAME_ZONE


FRAUDE
0
1
Proportion
MOYENNE_MONTANT_J_30J


FRAUDE
0
1
Count
MOYENNE_MONTANT_J_30J


FRAUDE
0
1
Proportion
MOYENNE_MONTANT_TRANSACTION_30J


FRAUDE
0
1
Count
MOYENNE_MONTANT_TRANSACTION_30J