ASJP Algerian Scientific Journal Platform

Revue afak Des Sciences
Issn: 2507-7228 – Eissn: 2602-5345
https://www.asjp.cerist.dz/en/PresentationRevue/351

Volume: 06/ N°: 04 (2021), P 608-617

Typologie de fraude aux Moyens de Paiement Electroniques Et Les Exigences Européennes de Sécurité

Types of Electronic Payment Fraud and European Security Requirements

Khelifa Mounia*
Universite khemis miliana
(Algeria)
mouniakh520@gmail.com

Abdelkader Khedaouimustapha
Universite khemis miliana
(Algeria)
mustaphalotfi62@yahoo.fr

Ladjlat Brahim
Université de Tissemsilt
(Algérie)
ladibr@gmail.com

Résumé:

Le développement des moyens de paiement électroniques est étroitement lié au développement des technologies de l'information et de la communication. Les innovations technologiques entraînent en parallèle une sophistication accrue des techniques de fraude, qui rend nécessaire une mise à niveau régulière des dispositifs de sécurité des systèmes attachés aux moyens de paiement.
Dans ce contexte, la sécurité des moyens de paiement est une exigence essentielle à la confiance que l'utilisateur porte pour ces moyens d'un cote et pour garantir la solvabilité et la stabilité des banques ; dans ce cadre on essaie de connaitre les types de fraudes appliques sur les moyens de payements électroniques et les démarches prises par l'union européennes pour faire faces a ces risques

informations sur l'article

Reçu
22 Mai 2021
Acceptation
22 Juin 2021

Mots clés:
- ✓ Les moyens de paiement électroniques ;
- ✓ La fraude ;
- ✓ la sécurité des opérations de paiement;

Abstract :

The development of electronic means of payment is closely linked to the development of information and communication technologies. Technological innovations are leading at the same time to an increased sophistication of fraud techniques, which makes it necessary to regularly upgrade the security devices of the systems attached to the means of payment.In this context, the security of means of payment is an essential requirement for the user's confidence in these means of payment and for guaranteeing the solvency and stability of banks; in this context, we try to know the types of fraud applied to electronic means of payment and the steps taken by the European Union to deal withtheserisks

Article info

Received
22 May 2021
Accepted
22 June 2021

Keywords:
- ✓ Electronic means of payment
- ✓ Fraud
- ✓ the security of payment transactions

* **Auteur expéditeur**

1. INTRODUCTION

L'adoption d'un moyen de paiement par les consommateurs relève d'un équilibre subtil entre le coût du moyen de paiement et sa facilité d'utilisation, d'une part, et les investissements devant être consentis par les prestataires de services de paiement pour en assurer la sécurité, d'autre part.

Un prestataire de services de paiement souhaitant commercialiser un nouveau moyen de paiement doit donc trouver un juste milieu entre ces deux impératifs. Le modèle économique qui en découlera devra en outre intégrer le coût de la fraude, dans la mesure où le prestataire de services de paiement sera susceptible de subir directement des pertes financières lors de la survenance d'attaques

Cette étude s'attache à clarifier :quelles sont les types de fraudes appliques sur les moyens de payements électroniques et les démarches prises par l'union européennes pour faire faces a ces risques ?

Cette étude est divisée sur 6 points essentiels détailles comme suit :

1- Les prestataires de services de paiement (PSP) ;

2- La notion de fraude aux moyens de paiement Electroniques ;

3- Typologie de la fraude observée ;

4- - les Techniques de fraude aux moyens de Paiement;

5- 5- Les modes opératoires utilisés par les fraudeurs

6- Les Exigences Européennes de Sécurité de Moyens de Paiement Electroniques

En premier lieu il faut savoir qui sont les prestataires de services de paiement ?

1. Les prestataires de services de paiement (PSP):sont les établissements habilités à tenir des comptes de paiement pour le compte de leur clientèle et à émettre des moyens de paiement. Ils relèvent des statuts suivants au sens des réglementations européennes :
   - 1.1 Etablissements de crédit ou assimilés, établissements de monnaie électronique et établissements de paiement et prestataires de services d'information sur les comptes[1];
   - 1.2 Etablissements de crédit, établissements de monnaie électronique et établissements de paiement et prestataires de services d'information sur les comptes droits étrangers. Paiement et infrastructures de marché à l'ère digitale

La valeur ajoutée d'un moyen de paiement du point de vue de l'utilisateur, peut se résumer par trois caractéristiques :

- 1.2.1 Sa simplicité d'utilisation,

1.2.2 Son faible coût voire sa gratuité,

1.2.3 Sa sécurité.

Deux risques principaux sur ce dernier point, sont généralement perçus par l'utilisateur :

- Le détournement des fonds en cours de paiement, susceptible d'entraîner une fraude immédiate,
- La captation des données bancaires de l'utilisateur qui pourrait entraîner des fraudes ultérieures

L'utilisateur se détournera d'un moyen de paiement présentant des failles de sécurité qu'il juge excessives, mais il préférera également s'abstenir si les méthodes utilisées pour sécuriser le moyen de paiement se traduisent par une trop grande complexité d'utilisation ou par un coût de transaction trop élevé, ce qui laisse une marge de manœuvre relativement limitée pour le développement de techniques avancées de sécurisation

Il peut exister un écart entre la sécurité réelle d'un moyen de paiement et la perception qu'en a l'utilisateur.Pour ce dernier, la sécurité du moyen de paiement sera souvent liée à une absence de perte financière pour lui, et non à l'impossibilité de réaliser des fraudes.

Dans certains cas, il peut ressortir de cette analyse qu'un risque de fraude accepté mais maîtrisé s'avérera commercialement plus rentable pour le prestataire de services de paiement et plus acceptable par les utilisateurs de son moyen de paiement que la mise en place de mesures permettant d'assurer, à l'extrême, une disparition quasi-totale du risque de fraude au prix d'une complexification excessive du « parcours client » susceptible de faire échouer l'acte de paiement

2. **La notion de fraude aux moyens de paiement Electroniques :**La fraude aux moyens de paiement est définie ici de manière plus restrictive comme recouvrant uniquement les utilisations illégitimes d'un moyen de paiement électroniques ou des données qui lui sont attachées, ainsi que tout acte concourant à la préparation ou à la réalisation d'une telle utilisation2Ayant pour conséquence un préjudice financier : ce préjudice peut affecter l'établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire du moyen de paiement électroniques , le bénéficiaire légitime des fonds (l'accepteur et/ou créancier), un assureur, un tiers de confiance ou tout intervenant dans la chaîne de conception, de fabrication, de transport, de distribution de données physiques ou logiques, dont la responsabilité civile, commerciale ou pénale pourrait être engagée;

2.2. Quel que soit le mode opératoire retenu, c'est-à-dire quels que soient :

2.2.1. Les moyens employés pour récupérer, sans motif légitime, les données ou le support du moyen de paiement (vol, détournement du support ou des données, piratage d'un équipement d'acceptation, etc.);

2.2.2. Les modalités d'utilisation du moyen de paiement ou des données qui lui sont attachées (paiement/retrait, en situation de proximité ou à distance, par utilisation physique de l'instrument de paiement ou des données qui lui sont attachées, etc.);

2.2.3. La zone géographique d'émission ou d'utilisation du moyen de paiement ou des données qui lui sont attachées.

2.3. Quelle que soit l'identité du fraudeur : un tiers, l'établissement teneur de compte et/ou émetteur du moyen de paiement, le titulaire légitime du moyen de paiement, le bénéficiaire légitime des fonds, un tiers de confiance, etc.

3. **Typologie de fraude aux Moyens de Paiement Electroniques**:

L'identification des techniques de fraude est, par nature, un objectif permanent dans la mesure où les fraudeurs cherchent de nouvelles failles au fur et à mesure de l'évolution des dispositifs de sécurité. De même, le renforcement des moyens de prévention de la fraude dans un secteur du marché des Paiement peut se traduire par un report de la fraude vers d'autres supports moins sécurisés ou vers d'autres zones géographiques[3].

On distingue quatre grandes typologies de fraude aux différents instruments de paiement :

3.1. **Faux** : fraude par établissement d'un faux ordre de paiement soit au moyen d'un instrument de paiement physique perdu, volé ou contrefait, soit via le détournement des données ou d'identifiants bancaires;

3.2. **Falsification** : fraude par utilisation d'un instrument de paiement falsifié (instrument de paiement authentique dont les caractéristiques physiques ou les 2 EMV (Pour Europay, Mastercard, VISA)[4] est un standard international de sécurité des cartes de paiement à puce, dont les spécifications ont été développées par le consortium EMVCo regroupant American Express, JCB Cards, Mastercard et Visa. Le standard EMV pour les Paiement de proximité et les retraits prévoit notamment le recours à la combinaison d'une puce sécurisée sur la carte associée à la saisie d'un code confidentiel, communément dénommée « chip & PIN ». 42 – Paiement et infrastructures de marché à l'ère digitale Chapitre 3 La sécurité des moyens de paiement données attachées ont été modifiées par le fraudeur) ou par altération d'un ordre de paiement régulièrement émis en modifiant un ou plusieurs de ses attributs (montant, devise, nom du bénéficiaire, coordonnées du compte du bénéficiaire, etc.);

3.3. **Détournement** : fraude visant à utiliser un instrument de paiement ou l'ordre de paiement sans altération ou modification d'attribut (à titre d'exemple, un fraudeur encaisse un chèque non altéré sur un compte qui n'est pas détenu par le bénéficiaire légitime du chèque);

3.4. **utilisation /contestation abusive** : fraude par répudiation abusive par le titulaire légitime du moyen de paiement d'un ordre de paiement qu'il a régulièrement émis. Utilisée dans le cadre des collectes statistiques mises en œuvre par la Banque de France au niveau national, cette typologie sert de socle commun à l'analyse de la fraude par les prestataires de services de paiement[5].

Selon les objectifs poursuivis, cette typologie peut être complétée par une analyse:

3.4.1. **du moyen de paiement ciblé** : carte de paiement, virement, prélèvement, chèque, autres instruments;

3.4.2. **des canaux de paiement utilisés** : paiement de proximité réalisé au poide vente grâce à un terminal de paiement ou sur un automate, paiement à distance sur internet, par courrier, par téléphone ou par tout autre canal;

3.4.3. **du préjudice et de sa répartition entre la banque du bénéficiaire**: la banque du payeur, le commerçant, le titulaire du moyen de paiement, les éventuelles assurances, les autres acteurs impliqués;

3.4.4. **du secteur d'activité du commerçant ayant fait l'objet de la fraude pour les Paiement à distance** : alimentation, jeux en ligne, services aux particuliers, produits techniques et culturels, télé- phonie et communication, etc.;

3.4.5. **des zones géographiques d'émission ou d'utilisation des moyens de paiement ou des données qui lui sont attachées**: selon que les banques du payeur et du bénéficiaire sont toutes deux établies dans le même pays ou la même zone monétaire ou pas. Nt

4. **Les Techniques de fraude aux moyens de Paiement**:

Un point central de toute analyse de la fraude est l'identification du mode opératoire utilisé par les fraudeurs. Avec le développement des moyens de paiement électroniques, les fraudeurs ciblent de manière croissante les données liées aux moyens de paiement ou à un service de paiement particulier[6].

Une difficulté réside dans le fait que ces données sont véhiculées tout au long de la chaîne de paiement. Cela nécessite par conséquent de déployer des dispositifs efficaces de protection sur l'ensemble de la chaîne et notamment sur tous les points sensibles identifiés.

4.1. **Les systèmes d'information** : il s'agit notamment des équipements informatiques (ordinateurs, Smartphones, etc.) des consommateurs ou des commerçants, des bases de données des prestataires de services de paiement et des concentrateurs monétiques pour les transactions liées à des cartes de paiement, qui peuvent être victimes d'attaques visant à capturer les données insuffisamment sécurisées.

À ce titre, les bases de données constituées aux différents stades de la transaction, et concentrant les données relatives à un grand nombre d'opérations, sont devenues très attractives pour les fraudeurs du fait de l'importance du volume des données susceptibles de faire l'objet d'une utilisation à des fins de fraude.

Pour être réalisée ; ce type d'attaque nécessite l'installation préalable de logiciels malveillants ou **« malwares »** à l'insu de l'utilisateur, ces logiciels étant généralement inoculés au travers de sources apparemment de confiance.

Cette technique de fraude vise tant les serveurs des grandes entreprises que les ordinateurs personnels des particuliers, et de manière croissante les téléphones mobiles qui sont de plus en plus utilisés dans le cadre de transactions de paiement. L'un des « malwares » les plus répandus, connu sous le nom de **« keylogger »**, permet ainsi d'enregistrer les touches frappées au clavier par la victime.

4.2. **Internet :** un fraudeur peut inciter les utilisateurs à communiquer leurs données personnelles telles que les données d'une carte de paiement (numéro de carte, date de validité, cryptogramme visuel situé au dos de la carte) ou d'authentification (par exemple, le numéro de téléphone mobile sur lequel sont envoyés les codes nécessaires à la confirmation d'une opération de paiement).

4.2.1. **L'hameçonnage** ou le « **phishing** ». est une technique de fraude qui repose généralement sur l'envoi de courriels usurpant des logos et chartes visuelles connus de leurs destinataires (par exemple un établissement de crédit) et invitant les victimes à se connecter à un site qui s'avère frauduleux, dont l'objet est de collecter des informations sensibles.

le fraudeur utilise Des variantes existent également sur téléphone mobile (« **vishing** »)[7], par lesquelles à des fins frauduleuses telles que des messages de type SMS, MMS ou notification

du système d'exploitation mobile.

4.2.2. **Le dévoiement** ou «**pharming** » :consisteà manipuler les serveurs afin de rediriger l'internaute, sans qu'il s'en aperçoive, vers un site frauduleux, en apparence semblable au site légitime, afin de collecter frauduleusement des fonds ou des données sensibles par ce biais.

4.2.3. **Les courriels, fax et conversations téléphoniques** : dans le cadre de transactions initiées par courrier, fax ou téléphone comportant une part de traitement manuel, des opérateurs mal intentionnés peuvent enregistrer les données bancaires lors d'un paiement ou d'une réservation en vue de les réutiliser ultérieurement.

4.2.4. **Les systèmes d'acceptation ou les réseaux :** pour les Paiement par carte, le matériel d'acceptation (automates de paiement ou de retrait et terminaux de paiement) ainsi que les réseaux véhiculant les données entre celui-ci et les serveurs d'acquisition peuvent être la cible d'attaques visant à s'approprier des donné

5. Les modes opératoires utilisés par les fraudeurs :

5.1. **.-Latechnique utilisée la plus fréquemment** consiste à capturer, à l'insu des porteurs[8], les données écrites sur les pistes magnétiques des cartes «skimming ». L'ensemble de la façade de l'automate ou sa fente d'insertion peuvent être factices et dissimuler le matériel illégitime.

Le dispositif est en outre associé à une caméra vidéo ou à un faux clavier permettant la capture du code confidentiel. Il peut également contenir des systèmes de stockage ou de transmission des données compromises.

5.2. **-Une autre technique** consiste à retenir une carte de paiement dans un automate afin de la réutiliser ultérieurement. À cette fin, le fraudeur insère un dispositif dans l'automate, observe la frappe du code confidentiel au clavier, puis il prend possession de la carte après le départ du porteur. Cette technique s'apparente à un vol physique de cartes de paiement.

5.3. **-Un fraudeur peut également exploiterdes failles de sécurité sur les éléments logiques des automates ou terminaux**. L'objectif est alors d'injecter un code malveillant dans les systèmes de ces matériels afin d'en modifier le comportement, voire de prendre le contrôle de leurs différents composants (clavier, écran et imprimante). Enfin, les réseaux eux-mêmes peuvent être la cible d'attaques lors de l'échange des données entre les matériels d'acceptation, les concentrateurs monétiques le cas échéant et les serveurs acquéreurs.

5.4. **Le vol physique du moyen de paiement** pour l'utiliser en lieu et place de son porteur légitime constitue le principal type d'attaque. Dans le cas des cartes, afin d'optimiser la fraude, le fraudeur tente en général de récupérer le code confidentiel de la carte, ce qui lui permet, à la fois, l'utilisation de la carte dans les distributeurs automatiques de billets, dans les terminaux de paiement et sur Internet, pour tous types de transactions.

Tableau (01):Les grandes typologies de fraude aux différents instruments de paiement

Typologie de Fraude	Carte de Paiement	Chèque	virement	Prélèvement
Faux	• Utilisation par le fraudeur d'une carte perdue ou volée à son titulaire légitime ou d'un numéro de carte usurpé (vente à distance) • Fausse carte créée par un fraudeur àpartir de donnéesqu'il a recueillies	• Utilisation parle fraudeur d'unchèque perduou volé à sontitulaire légitime • Faux chèque, crééde toutes piècespar un fraudeur,émis sur unebanque existante ouune fausse banque	• Transmission par lefraudeur d'un fauxordre de virement • Usurpation desinformationsde connexionà un espacebancaire en lignepour initier desvirements frauduleux	• Émission par lefraudeur d'un ordrede prélèvementsans mandatou à partir d'unfaux mandat
Falsification	• Carte authentiquedont les donnéesmagnétiques, d'embossage a) oude programmationont été modifiéespar le fraudeur	• Chèque régulier intercepté par le fraudeur qui l'altère par grattage gommage ou effacement	• Virement régulierintercepté etmodifié parle fraudeur	• Remplacementdes référencesdu compte ducréancier légitimepar celles ducompte dufraudeur sur unordre ou fichierde prélèvement
Détournement	• Paiement ou retrait sous la contrainte	• Chèque réguliersigné par le titulaire légitime sous la contrainte ou la manipulation	• Virement initié, parle titulaire légitimedu compte, sous lacontrainte ou par latromperie vers uncompte qui n'est pascelui du bénéficiairelégitime ou qui necorrespond à aucuneréalité économique	• Usurpation parle fraudeur del'identité etl'IBAN d'un tierspour la signatured'un mandat deprélèvement sur uncompte qui n'estpas le sien
Utilisation/contestation abusive	• Contestation abusivepar le porteurd'une transactionde paiementpar carte validequ'il a initiée	• Chèque émis par letitulaire légitime, demanière abusive, àpartir d'une formuleauthentique qu'ila préalablementdéclarée perdueou volée	• Contestationabusive par letitulaire du compted'un ordre devirement validequ'il a initié	• Contestationabusive par ledébiteur d'un ordrede prélèvementémis légitimementpar le créancier(litige commercial)

Source: La sécurité des paiements en ligne va être renforcéeParGéraldine Houdayer,France Bleuhttps://www.francebleu.fr/infos/societe/la-securite-des-paiements-en-ligne le 21/03/2020

6. **Les Exigences Européennes de Sécurité de Moyens de Paiement Electroniques** : pour assurer la sécurité de ses moyens de paiement les pays européens ont mises en place au niveau le respect des droits des utilisateurs des moyens de paiement Electroniques

6.1. **La Sécurité des Systèmes d'Information**: Les dispositifs de lutte contre la fraude doivent intégrer en priorité la protection des données à caractère personnel. Les systèmes d'information doivent ainsi répondre à des standards de sécurité permettant de limiter les risques identifiés de captation des données liées aux moyens de paiement.

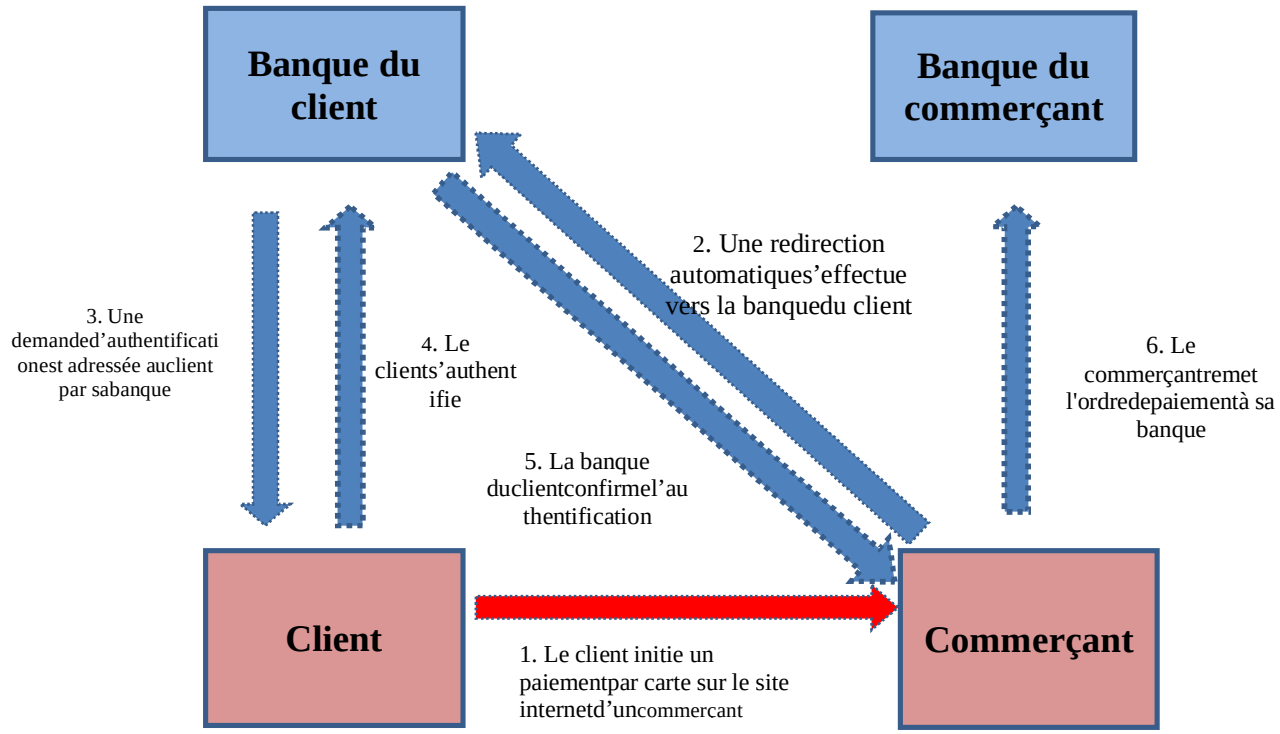
D'une manière générale les systèmes d'information doivent, , être protégés contre les menaces internes ou externes et faire l'objet, à ce titre, d'analyses

de sécurité visant à mettre en place des mesures de protection adaptées au contexte dans lequel ils évoluent. Leurs gestionnaires doivent ainsi définir une politique de sécurité et réévaluer régulièrement les risques auxquels ils sont exposés. Différentes méthodes leur sont proposées.

6.2. **En matière d'attaque contre les bases de données**, la directive européenne sur la sécurité des réseaux et de l'information dans l'Union[9], adoptée le 6 juillet 2016, impose en particulier aux banques ainsi qu'aux e-commerçants de mettre en place **des systèmes de protections** de leurs données adaptés aux risques évalués et de déclarer aux autorités les violations de leurs bases de données contenant des informations sur la clientèle et notamment des informations sur les moyens de paiement.

6.3. **La sécurité des données au moment de leur enregistrement dans les systèmes** doit également faire partie intégrante de ces politiques de sécurité. Celles-ci doivent en effet prévoir une traçabilité de l'ensemble des accès au système d'information ayant pour objet la saisie ou la modification de données nécessaires à la réalisation de la transaction, afin de constituer une piste d'audit fiable. Les compromissions généralement constatées dans ce contexte relèvent de malversations initiées par du personnel indélicat.

Schemat N 01 : Les Procédures de la Sécurité des Cartes de paiement



Source :Rapport de l'Observatoire de la Sécurité des Cartes de paiement, 2010https://www. banque-france.fr/sites Consulte 20/04/2020

6.4. **Des dispositifs d'acceptation limitant l'interaction entre les commerçants et les moyens de paiemen**t doivent donc être privilégiés. Il est en outre important de limiter l'accès aux données au seul personnel réellement habilité et de ne pas conserver de données sensibles dès lors que celles-ci ne sont plus utiles[10].

6.5. **La sensibilisation des utilisateurs**:La sensibilisation des utilisateurs aux questions de sécurité est indispensable, notamment pour lutter contre les attaques

frauduleuses. **Une communication efficace**, utilisant l'ensemble des canaux disponibles (courriers, courriels, sites Internet, etc.), est donc souhaitable de la part de l'ensemble des acteurs de la chaîne de paiement doit donc être instaurée afin d'attirer la vigilance des utilisateurs sur les facteurs de risque et les bonnes pratiques à respecter.

Les utilisateurs doivent en outre être incités à n'utiliser que des sites de confiance, dont le niveau de sécurité apparaît conforme aux termes de référence cités dans ces communications.

L'identification des transactions à risque La mise en place de dispositifs reposant sur l'analyse et l'exploitation des données personnelles du payeur constitue un axe de développement clef dans la détection des transactions frauduleuses.

7. *Conclusion*:

D'une année à l'autre, les dispositifs de sécurité des moyens de paiements électroniques ont eu tendance à élargir le nombre et la nature des données collectées lors d'une transaction sur Internet afin de vérifier la cohérence entre ces données et d'augmenter le degré de certitude quant à l'identité de la personne initiant la transaction de paiement. Ainsi, aux côtés des données traditionnellement collectées relatives à l'identité et aux coordonnées**.**

Les nouveaux moyens de paiement étant plus sûrs, il faut désormais s'intéresser à l'étape d'après, à savoir le traitement de la data. Les banques devront investir sur 3 sujets clés :

- Assurer la sécurité des données personnelles. Le renforcement du contexte réglementaire, à la faveur de l'entrée en vigueur du RGPD (règlement général sur la protection des données)
- Garantir la transparence de l'utilisation des données. .
- Sensibiliser les clients aux différents risques, notamment ceux concernant les données transmises volontairement aux entreprises et services sur Internet. La révolution de la banque digitale tient surtout à la démocratisation des usages d'internet. Il est donc de la responsabilité des banques d'informer les utilisateurs.

Liste Bibliographique: (APA)

- AfterbankingPaul De Leusse, 2019banque et confiance : la grande réconciliation digitale - Collection Sens
- Paul De Leusse ;2019;Afterbanking Banques et confiance ; Débats Publics
- Jean-François Hamelin; 2021;Le financement dans tous ses états ; Juris éditions
- Sokrou Adélaïde;Gakoué,2020 « Fraude à la carte bancaire et paiement en ligne : quelle garantie de sécurité ? », Doc Publication, Les Editions de l'Immatériel, article sur site internet ttps://www.capitaine-banque.com › actualite-banque › fr consulte le 28/05/2020
- capitaine-banque.com,2020, Que faire en cas de fraude bancaire ? - Capitaine Banque, article sur site internet https://www.capitaine-banque.com › actualite-banque › fr.consulte . le09/05/2020
- Géraldine Houdayer, France Bleu,2019,**l**a sécurité des paiements en ligne va être renforcéearticle publie sur site internet,https://www.francebleu.fr/infos/societe/la-securite-des-paiements-en-ligne-va-etre-renforcee consulte 11 septembre 2019
- leparisien.fr, 2021, Paiements en ligne et sans contact : les fraudes se multiplient article publie sur site internet.https://www.leparisien.fr › Economie › Gerer-son-budget ; consulte le 25 avril 2021
- Géraldine Houdayer, France Bleu,2020,La sécurité des paiements en ligne va être renforcée,https://www.francebleu.fr/infos/societe/la-securite-des-paiements-en-ligne le 21/03/2020
- banque-france.fr, 2010, Rapport de l'Observatoire de la Sécurité des Cartes de paiement, 2010,https://www. banque-france.fr/sites28/04/2020

1. Géraldine Houdayer, France Bleu,2020, La sécurité des paiements en ligne va être renforcée Par https://www.francebleu.fr/infos/societe/la-securite-des-paiements-en-ligne le 24/03/2020
2. banque-france.fr, rapport annuel 2017 de l'Observatoire de la sécurité des moyens de paiement, https://www.banque-france.fr/ consulte le 20/03/2020
3. ecb.europa.eu,2020,Oversight framework for cardpaymentscheme standards, January 2008,http://www.ecb.europa.eu/pubopcit consulter le 21/03/2020

6. *Annexes :*

1AfterbankingPaul De Leusse, banque et confiance : la grande réconciliation digitale - Collection Sens 2019 p 44

2AfterbankingPaul De Leusse, banque et confiance : la grande réconciliation digitale - Collection Sens 2019 opcit p 45

3 La sécurité des paiements en ligne va être renforcée Par Géraldine Houdayer, France Bleuhttps://www.francebleu.fr/infos/societe/la-securite-des-paiements-en-ligne le 21/03/2020

4 Rapport de l'Observatoire de la Sécurité des Cartes de paiement, 2010https://www. banque-france.fr/sites28/04/2020

5 Source : La sécurité des paiements en ligne va être renforcée Par Géraldine Houdayer, France Bleuhttps://www.francebleu.fr/infos/societe/la-securite-des-paiements-en-ligne le 24/03/2020

6La sécurité des paiements en ligne va être renforcéePar Géraldine Houdayer, France Bleuhttps://www.francebleu.fr/infos/societe/la-securite-des-paiements-en-ligneopcit consulter le 21/03/2020

7rapport annuel 2017 de l'Observatoire de la sécurité des moyens de paiement, https://www.banque-france.fr/ consulte le 20/03/2020

8Oversight framework for cardpaymentscheme standards, January 2008,http://www.ecb.europa.eu/pubopcit consulter le 21/03/2020

9Stabilite-financiere/observatoire-de-la-securite-des-moyens-de-paiement site https://www.banque-france. Consulte le 28/05/2020

10Stabilite-financiere/observatoire-de-la-securite-des-moyens-de-paiement site https://www.banque-france. Consulte le 20/05/2020 opcit.