Évolution de la nature et de l'échelle des risques que présentent les SFN pour le consommateur Examen des faits

CGAP

FÉVRIER 2022

Majorie Chalwe-Mulenga, Eric Duflos, et Gerhard Coetzee

REMERCIEMENTS

Les auteurs tiennent à remercier les experts dont la liste figure en annexe pour leurs précieux conseils dans le cadre de la présente étude. Ils expriment également leur gratitude à Barbara Scola et à Ivo Jenik pour la relecture de cette série de diapositives, à Juan Carlos Izaguirre pour ses idées, ainsi qu'à Natalie Greenberg, Lamis Daoud et Jahda Swanborough pour leur appui lors de la rédaction de cette étude.

GROUPE CONSULTATIF D'ASSISTANCE AUX PAUVRES

1818 H Street NW, MSN F3K-306
Washington DC 20433
Site Internet : www.cgap.org
Courriel : cgap@worldbank.org
Téléphone : +1 202 473 9594

Couverture : Photo pour le CGAP de Lorena Velasco via Communication for Development Ltd.

DROITS ET LICENCES

TABLE DES MATIÈRES

RÉSUMÉ ANALYTIQUE

L’évolution des risques dans les services financiers numériques

Les services financiers numériques (SFN) ont indéniablement induit des avantages considérables sur le plan de l'inclusion financière et contribué énormément à la croissance économique et au développement. Parmi les effets positifs que les SFN ont sur leurs utilisateurs, on peut citer l’amélioration des comportements en matière d'épargne, l'autonomisation grâce à une plus grande confidentialité et la capacité à mieux résister aux chocs. Parallèlement, les SFN ont exacerbé les risques existants pour les consommateurs et continuent d'introduire de nouveaux risques qui évoluent sans cesse, eu égard au caractère dynamique de la technologie financière. Ces risques compromettent la prestation des SFN aux utilisateurs mal desservis et ceux à faible revenu et vont probablement, s'ils sont ignorés, saper la confiance des consommateurs à l’égard de ces services.

Nos objectifs et notre méthodologie

En octobre 2020, le Groupe consultatif d’assistance aux pauvres (CGAP) a engagé des recherches pour appréhender **l'évolution de la nature et de l’ampleur des risques que les SFN présentent pour les consommateurs** dans le cadre de notre action de protection des consommateurs.

La recherche vise à déterminer les nouveaux risques qui ont émergé pour les utilisateurs de SFN à la suite de la note d'information 2015 du CGAP, intitulée Réussir la finance numérique : pourquoi atténuer davantage les risques pour les clients, et à créer une typologie des risques conforme à cette évolution. Nous avons aussi voulu nous faire une idée de la mesure dans laquelle les risques que les SFN présentent pour les utilisateurs ont augmenté ou diminué au cours des dernières années. Nous croyons que cette information est essentielle pour les parties prenantes qui souhaitent bâtir un écosystème responsable de SFN.

Reconnaissant que certains segments de clientèle sont plus vulnérables que d’autres aux risques que présentent les SFN pour le consommateur, notre exposé met en évidence les risques qui touchent les consommateurs vulnérables, en particulier les femmes à faible revenu et les populations rurales, et se penche sur la façon dont le surendettement peut résulter d'une combinaison de risques associés aux SFN.

L’exposé résume les constatations de notre recherche, qui est fondée sur un examen de plus de 170 publications, ainsi que sur des consultations avec 74 experts de 33 organisations, comme il est indiqué en détail dans l’annexe.

RÉSUMÉ ANALYTIQUE

Quel est le public ciblé par la présente série de diapositives ?
L'exposé vise à fournir à diverses parties prenantes, notamment aux décideurs, aux organismes de réglementation, aux organismes de supervision, aux bailleurs de fonds, aux associations de consommateurs et aux fournisseurs de SFN, un cadre complet concernant l'évolution de la nature et de l'échelle des risques que les SFN présentent pour les consommateurs. Chaque acteur joue un rôle dans la sensibilisation des clients aux risques, et à la capacité de les éviter. Notre exposé décrit également les mesures proactives que les diverses parties peuvent prendre pour atténuer les risques et veiller à ce que les consommateurs continuent de faire confiance aux SFN.

Les SFN ont fait apparaître plusieurs nouveaux risques pour les consommateurs, notamment la fraude par application mobile, l'usurpation d'identité synthétique, les arnaques au paiement par autorisation et les risques liés à l'intelligence artificielle, tels que le biais algorithmique. Parallèlement, **les risques préexistants pour les consommateurs** tels que la fraude par échange de cartes SIM, les violations de données, les arnaques par ingénierie sociale et les pyramides de Ponzi **sont devenus plus complexes.**

Nous avons répertorié 66 risques pour les consommateurs de SFN qui sont regroupés en :

- **quatre grands types de risque**, à savoir la fraude, l'utilisation abusive des données, le manque de transparence et l'inadéquation des mécanismes de recours ;
- **deux types de risques transversaux** : les risques liés aux agents et les pannes de réseau.

Nous avons examiné d'autres typologies des risques, décrites dans l'annexe, mais nous nous sommes limités à la typologie que nous avons choisie, eu égard à sa simplicité.

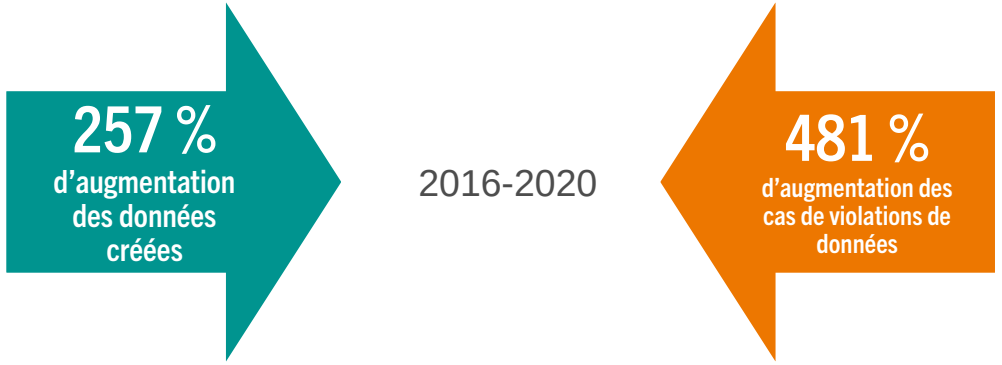
Il convient de noter que la fraude, l'utilisation abusive des données et certaines pannes de réseau, tout comme des risques liés aux agents, sont directement liés à la **cybersécurité.** De plus, les deux types de risques transversaux que les SFN présentent pour les consommateurs – en l'occurrence les risques liés aux agents et les pannes de réseau – entravent la fourniture de SFN aux consommateurs peu desservis et démunis.

RÉSUMÉ ANALYTIQUE

Certains risques prennent le pas sur les avancées technologiques et l'adoption des SFN. Les données disponibles font apparaître une très forte augmentation du nombre de cas de violations de données. À cela s'est ajoutée la multiplication d'actes criminels tels que la fraude par application mobile, la fraude par échange de cartes SIM, les prises de contrôle de comptes et les fraudes par les réseaux sociaux. Des données empiriques indiquent par ailleurs que le manque de transparence s'est fortement accentué, alors que les mécanismes de recours ont été à peine améliorés dans certains pays.

50 % des entreprises ont accru leur dispositif d'accompagnement des clients en 2020, mais seulement **25 %** des clients ont reçu des réponses plus rapides à leurs requêtes ou ont été capables de se connecter à ce service proposé à la clientèle

Source : Rapport d'Experian sur l'usurpation d'identité et la fraude dans le monde, 2021



Source : Statista (données créées dans le monde) ; rapport de fin d'année 2020 de Risk Based Security (nombre mondial de cas de violations de données)

Source : Rapport Outseer sur la fraude et les paiements, T1 2018 et T2 2021

RÉSUMÉ ANALYTIQUE

Les femmes à faible revenu et les populations rurales ont de fortes chances d'être plus exposées aux risques que les SFN présentent pour les consommateurs. S'il est vrai que les femmes à faible revenu et les populations rurales sont confrontées aux mêmes risques que les autres utilisateurs, il n'en demeure pas moins que leur faible culture numérique couplée à leurs compétences financières limitées accentue leur vulnérabilité aux risques que présentent les SFN. Les femmes rurales sont les plus exposées à ces risques. Les femmes et les populations rurales font face à des risques tels que la fraude imputable à l'agent et le fait qu'elles n'utilisent pas des interfaces téléphoniques complexes. Les normes sociales peuvent aussi limiter la capacité des femmes à se plaindre des problèmes causés par les SFN. En outre, les femmes et les populations rurales sont plus susceptibles de partager leurs téléphones ou leurs codes PIN avec d'autres personnes. Compte tenu de la rareté des données désagrégées, nous n'avons pas pu évaluer l'évolution des risques qui touchent les femmes et les populations rurales.

Une combinaison de plusieurs risques pour les consommateurs peut entraîner un surendettement. Les données disponibles montrent que des plateformes numériques telles que les applications mobiles et les plateformes de prêt de particulier à particulier (P2P) ont exposé les consommateurs à des risques qui déboucheront sur une situation de surendettement. Les applications numériques et plateformes de prêt P2P non autorisées, qui imitent les applications et plateformes authentiques, obtiennent de façon intrusive des informations sur les clients et offrent aux clients désespérés des prêts numériques sans tracas, mais coûteux. Les agents recourent ensuite à des pratiques de recouvrement excessives, telles que l'intimidation des clients pour faire pression sur eux et les amener à rembourser leurs prêts. Compte tenu de l'inadéquation des mécanismes de recours, les clients ne peuvent pas renégocier leurs prêts et doivent recourir à des stratégies d'adaptation négatives, par exemple obtenir des prêts supplémentaires pour racheter leurs créances ou réduire leurs achats de denrées alimentaires.

Il y a un besoin urgent de mesures proactives qui maintiennent la confiance des clients dans les SFN et assurent des résultats positifs. Les organismes de réglementation et de supervision peuvent élaborer des systèmes pour détecter et surveiller les risques. Ils peuvent également recueillir des données désagrégées et mettre en place des mécanismes de coordination pour collaborer avec d'autres agences de régulation du secteur. Les bailleurs de fonds et les investisseurs peuvent intégrer l'analyse des risques qui pèsent sur les consommateurs dans la conception des projets de SFN. Les fournisseurs de SFN peuvent concevoir des services axés sur le client qui renforcent la solidité financière des prestataires de ces services tout en induisant des résultats positifs pour les clients. Les groupes de consommateurs peuvent susciter une prise de conscience des clients et alerter les superviseurs au sujet des risques, alors que les chercheurs peuvent continuer à combler les lacunes mises en évidence dans la présente étude. Pour plus d'informations, consulter le guide pratique de surveillance du marché, le travail de recherche intitulé Collective Consumer Voice et la page du guide du CGAP axé sur le client, intitulée Customer-Centric Guide [en anglais].

I. AVANTAGES DES SERVICES FINANCIERS NUMÉRIQUES (SFN)

LES SFN CRÉENT DES POSSIBILITÉS QUI PEUVENT CHANGER LA VIE DE LEURS CONSOMMATEURS

Les SFN aident les utilisateurs à épargner, à emprunter et à recevoir des transferts de fonds – réduisant du même coup les mécanismes d'adaptation négatifs

Effets positifs que les SFN ont sur les usagers

- ✓ L'amélioration du comportement en matière d'épargne
- ✓ L'autonomisation grâce à une confidentialité accrue
- ✓ Une économie financière et de temps
- ✓ Une meilleure capacité à faire face aux chocs et à récupérer plus rapidement
- ✓ Le lissage de la consommation

Source : carte des lacunes en matières de données de la Fondation Mastercard

Une étude menée en Ouganda a révélé que la probabilité d'épargner, d'emprunter et de recevoir des transferts de fonds augmentait de 25, de 22 et de 82 points de pourcentage, respectivement, dans les ménages qui utilisaient de l'argent mobile (Munyegera et Matsumoto 2017). Une autre étude a révélé que les femmes qui avaient reçu un prêt de microfinance sur leur compte d'argent mobile enregistraient des bénéfices commerciaux de 15 % plus élevés et des niveaux de capital commercial de 11 % plus élevés (Riley 2019).

Au Mexique, lorsque le programme Oportunidades a fait passer son système de paiement des espèces aux paiements électroniques, la fréquence de réception des transferts de fonds a augmenté et la participation à l'épargne informelle a diminué. Cette évolution a aussi réduit le recours à des stratégies d'adaptation négatives telles que la réduction de la consommation de denrées alimentaires (Masino et Niño Zarazúa 2014).

Un essai contrôlé randomisé mené au Bangladesh qui a introduit le paiement électronique des salaires à une population de salariés d'usine a augmenté les niveaux d'épargne et la capacité de faire face à des chocs imprévus (Breza et al. 2017).

Une évaluation au Kenya de l'adoption et de l'impact de M-shwari, l'un des produits de crédit numérique les plus populaires au monde, a révélé que les ménages qui utilisaient M-shwari avaient 6,3 % moins de chances de renoncer à des dépenses de base à cause de chocs négatifs (Bharadwaj et al. 2019).

Au Ghana, Tigo Family Care (Tigo), une assurance mobile semi-payante (« freemium ») lancée en 2010 a permis de faire passer du simple au double le volume du marché de l'assurance en moins de trois ans. Au début de 2013, Tigo avait étendu sa couverture de base de l'assurance vie à 978 000 personnes, bien plus que les 540 000 Ghanéens (5,4 % des adultes du pays) qui étaient couverts par une police d'assurance formelle en 2010 (Zetterli 2013).

LES SFN PEUVENT MÊME ÉLARGIR L'ACCÈS À DES SERVICES ESSENTIELS

Mais tous ces avantages peuvent être remis en cause par des risques. S'ils sont ignorés, les risques vont probablement saper la confiance des utilisateurs dans les SFN.

Nos recherches font ressortir des moyens prometteurs par lesquels la finance numérique peut aider à relever les défis en matière de développement.

La finance numérique peut accroître l'efficacité et faire apparaître de nouveaux modèles commerciaux tels que le paiement à l'utilisation (le « pay-as-you-go ») qui élargissent l'accès des ménages à faible revenu aux commodités essentielles comme l'électricité, l'eau et les combustibles pour la cuisson des aliments (Waldron et Sotiriou, 2019).

En Côte d'Ivoire, les conclusions d'une enquête expérimentale visant à évaluer les effets d'un produit numérique de prêts à court terme à l'éducation octroyés par l'intermédiaire de coopératives a révélé que ce produit a contribué à accroître le taux des enfants qui commencent l'école, en le faisant passer de 49 % à 73 % (Vidal et Barbon, 2018).

Cependant, les avantages des SFN peuvent être remis en cause par des risques qui, s'ils sont ignorés, vont probablement saper la confiance des utilisateurs dans les SFN.

Les consommateurs ont beaucoup à gagner des SFN, mais les possibilités qu'offrent ces services vont de pair avec les risques qui leur sont associés. Les risques perçus pour les consommateurs peuvent décourager les non-utilisateurs d'adopter les SFN. Les risques qui se matérialisent peuvent entraîner des pertes financières directes pour les utilisateurs, ainsi que d'autres préjudices susceptibles de saper leur foi et leur confiance dans les SFN.

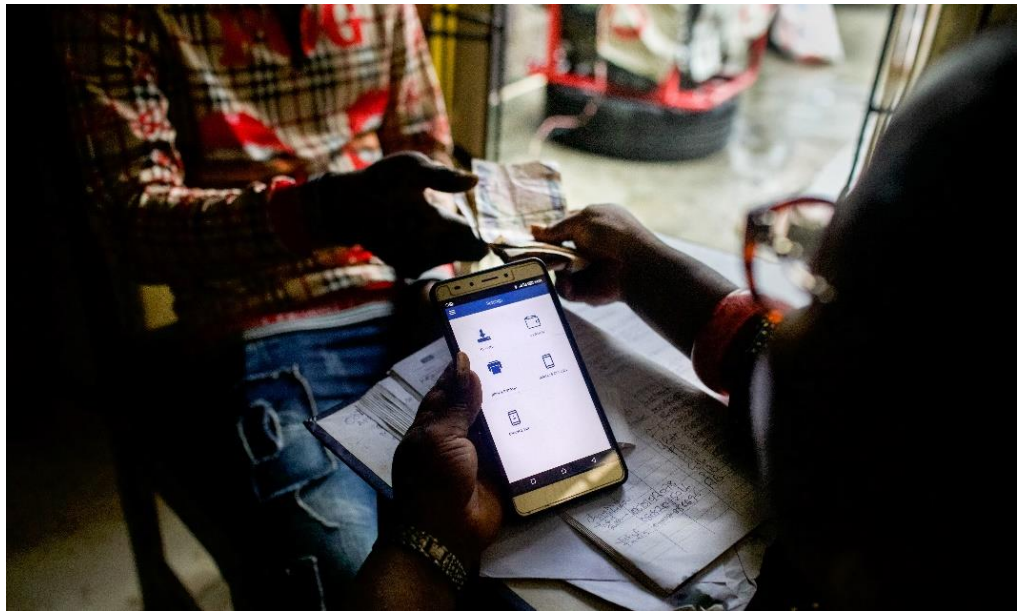


Photo pour le CGAP de Lorena Velasco via Communication for Development Ltd.

II. NOUVELLE TYPOLOGIE DES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

LES RISQUES ACTUELS SONT DEVENUS PLUS COMPLEXES

Les risques pour les utilisateurs de SFN ont augmenté avec le temps

Fraude par échange de cartes SIM. Même si la fraude par échange de cartes SIM constitue un problème mondial, elle est plus récurrente dans les pays en développement (Farooq, 2019). Il n'existe pour l'instant aucun élément factuel à l'échelle planétaire qui pourrait étayer l'évolution de ce risque, mais des données provenant d'Afrique du Sud montrent que la progression de la fraude par échange de cartes SIM était plus élevée que le taux de croissance de la pénétration de la téléphonie mobile (SABRIC, 2019 ; Outil DataBank de la Banque mondiale).

Violations de données. Le nombre de données divulguées a connu une augmentation impressionnante au cours des dernières années, associée à un accroissement des données générées par l'utilisation des médias sociaux et de l'Internet des objets. D'après les données disponibles, l'augmentation du nombre de dossiers divulgués croît à un rythme plus rapide que le taux de création de données.

Arnaques par ingénierie sociale. Les tactiques d'ingénierie sociale ne se limitent pas à l'hameçonnage (courriels frauduleux incitant les gens à révéler des informations personnelles, qui sont ensuite utilisées pour commettre une fraude), mais comprennent également l'hameçonnage par textos (SMS) et par appel vocal. L'hameçonnage par SMS et l'hameçonnage par appel vocal sont les principaux vecteurs de fraude utilisés pour cibler des personnes à faible revenu qui utilisent principalement les plateformes mobiles de SFN.

Les arnaques par ingénierie sociale ont été plus fréquentes ces dernières années, notamment depuis l'apparition de la pandémie de maladie à coronavirus 2019 (COVID-19) (Medine 2020). Une autre arnaque par ingénierie sociale en plein essor qui touche les utilisateurs de smartphones est la fraude par code de question rapide (QR), qui se produit lorsque des escrocs se servent de codes QR légitimes pour accéder aux données personnelles des clients et leur voler de l'argent.

Investissements numériques non agréés/pyramides de Ponzi. L'avènement des cryptomonnaies a conduit à l'émergence de pyramides de Ponzi basées sur les cryptomonnaies. Ces systèmes persuadent généralement les personnes à faible revenu qui n'ont pas les compétences nécessaires pour utiliser des plateformes cryptographiques complexes de transférer leurs fonds à des acteurs peu scrupuleux promettant d'investir en leur nom dans des actifs cryptographiques. Ces systèmes gagnent la confiance des personnes à faible revenu parce qu'ils fonctionnent sur le modèle des réseaux d'entraide (groupes d'épargne auxquels les personnes à faible revenu sont habituées).

Parmi les autres risques, on peut citer le risque lié au partage de responsabilités, les ventes abusives, les frais cachés et les pratiques abusives de recouvrement de dettes.

APPARITION DE NOUVEAUX RISQUES POUR LES UTILISATEURS DE SFN

Nous avons recensé cinq risques relativement nouveaux depuis que le CGAP a mené des recherches sur les risques pour les consommateurs de SFN en 2015

1. **Fraude par application mobile.** Compte tenu de l'adoption croissante des smartphones, la fraude par application mobile est globalement en hausse (RSA 2020 ; Fu et Mishra 2020a). La fraude par application mobile se produit lorsqu'un fraudeur utilise une application mobile malveillante pour tromper un client. L'étude Next Billion Users de Google estime que d'ici à 2025, l'on comptera un milliard de nouveaux utilisateurs de smartphones qui auront probablement des revenus plus faibles et un niveau d'éducation moins élevé, qui vivront dans des zones moins développées où l'Internet est moins fiable, qui seront peu exposés à la technologie et qui utiliseront les smartphones avec moins d'assurance. Si des mesures délibérées ne sont pas prises pour protéger les utilisateurs inexpérimentés, davantage de personnes seront exposées à la fraude commise au moyen d'applications mobiles.

2. **Fraude par identité biométrique.** Les données biométriques sont utiles pour atténuer les risques. Cependant, les fraudeurs peuvent obtenir des copies d'empreintes digitales ou des photos haute résolution pour accéder aux comptes des clients, les systèmes de sauvegarde des données biométriques peuvent être violés, et les vides juridiques peuvent conduire à une utilisation abusive des données (Stolba 2020 ; Medine 2017).

Selon Europol (2020a) « dans l'avenir, les forces de l'ordre et le secteur devront s'attendre à voir une utilisation accrue de la biométrie vocale pour commettre des fraudes par usurpation d'identité ».

3. **Arnaques au paiement par autorisation (APP).** Une arnaque au paiement par autorisation se produit lorsqu'un fraudeur incite un consommateur à envoyer de l'argent sur un compte contrôlé par des criminels. L'enquête menée à l'échelle mondiale par KPGM sur la fraude bancaire intitulée Global Banking Fraud Survey (2019b) note que les arnaques au paiement par autorisation ont augmenté entre 2015 et 2018 dans toutes les régions du monde (voir la diapositive 22). Le Royaume-Uni a signalé une hausse de 15 % du nombre de cas d'escroquerie au paiement par autorisation en 2020 (Michael et Smith 2021).

APPARITION DE NOUVEAUX RISQUES POUR LES UTILISATEURS DE SFN

Cinq risques relativement nouveaux ont été détectés depuis l'étude menée en 2015 par le CGAP

4. Usurpation d'identité synthétique. L'usurpation d'identité synthétique se produit lorsque « de nouvelles identités sont fabriquées en mélangeant des éléments provenant de plusieurs individus, ce qui rend la découverte de transactions frauduleuses plus compliquée » (FICO 2018). Ce type de fraude est un problème dont la sophistication, l'intensité et la fréquence augmentent (Aite Group 2021 ; FICO 2018). Les Federal Reserve Banks (2021) ont récemment élaboré une définition commune pour mieux doter les prestataires de services financiers des moyens d'identifier et d'atténuer l'usurpation par identité synthétique. L'usurpation d'identité synthétique est préoccupante, car, contrairement à d'autres types de fraude, elle peut toucher simultanément plusieurs clients et rendre difficile l'identification des personnes qui ont été touchées.

5. Risques liés à l'intelligence artificielle (IA). Si l'intelligence artificielle n'est pas une notion nouvelle, l'apprentissage autonome dans l'intelligence artificielle a introduit des risques plus nouveaux pour les utilisateurs de SFN, tels que le biais ou la discrimination algorithmique, la vente abusive, l'intrusion dans la vie privée et les prises de décisions opaques (Banque mondiale 2021 ; OCDE 2020a, 2020b ; Sahay et al. ; Dvara Research 2020 ; Chugh 2019 ; Francis et al. 2017 ; Hurly et Adebayo, 2017 ; Commission européenne 2016). Malheureusement, il n'existe actuellement aucun consensus sur les points de référence qui peuvent être utilisés pour mesurer ou évaluer la relation de l'intelligence artificielle avec des débats de société plus larges (Zhang, et al. 2021; Mishra et al. 2020).

LA PRÉSENTE ÉTUDE A PERMIS AU CGAP D'ÉLABORER UNE NOUVELLE TYPOLOGIE DE RISQUES POUR LES CONSOMMATEURS DE SFN

Catégorisation des risques liés aux SFN effectuée par le CGAP

Compte tenu de la nature dynamique des risques pour les utilisateurs de SFN, le CGAP a identifié 66 risques et les a regroupés en **quatre grands types de risques et deux types de risques transversaux**.

Quatre grands types de risques

FRAUDE

Exemples :
- Fraude par échange de cartes SIM
- Fraude par application mobile

USAGE ABUSIF DES DONNÉES

Exemples :
- Biais algorithmique
- Pratiques injustes (par exemple, l'intimidation sociale)

MANQUE DE TRANSPARENCE

Exemples :
- Frais cachés
- Complexité de l'interface utilisateur

INADÉQUATION DES MÉCANISMES DE RECOURS

Exemples :
- Complexité du processus de dépôt de plaintes
- Système onéreux de traitement des plaintes

Deux types de risques transversaux

RISQUES LIÉS AUX AGENTS
Exemples : problèmes de liquidité, fraude commise par les agents, discrimination selon le statut social

PANNE DE RÉSEAU
Exemples : attaques par déni de service distribué, mise à niveau des systèmes insuffisamment éprouvée, coupure de courant

Nous avons également constaté que la fraude et l'utilisation abusive des données sont directement liés à la cybersécurité, tandis que le manque de transparence et l'insuffisance des mécanismes de recours n'ont pas de lien direct avec la cybersécurité. Les deux risques transversaux partagent aussi certains éléments avec les quatre grands risques. Vous trouverez à l'annexe une liste détaillée des 66 anciens et nouveaux risques identifiés, ainsi que les définitions des quatre grands types de risques et des deux types de risques transversaux.

III. ÉVOLUTION DE L’ÉCHELLE DES RISQUES ASSOCIÉS AUX SFN*

* Pour d'autres exemples, voir l'annexe

L'ÉCHELLE DES RISQUES POUR LES UTILISATEURS DE SFN EST EN HAUSSE DANS LA PLUPART DES CAS

Les éléments factuels et données disponibles depuis 2015 montrent un accroissement d'échelle pour la plupart des types de risques répertoriés par le CGAP.

Type de risque	Monde	Régions*	Pays
1. Fraude*			
2. Utilisation abusive des données			
3. Manque de transparence			S. O.
4. Inadéquation des mécanismes de recours**	S. O.	S. O.	

Flèche rouge : les données disponibles montrent un accroissement **général** en valeur ou en volume

Flèche orange : la documentation indique un accroissement en valeur ou en volume sans bases de données d'appui.

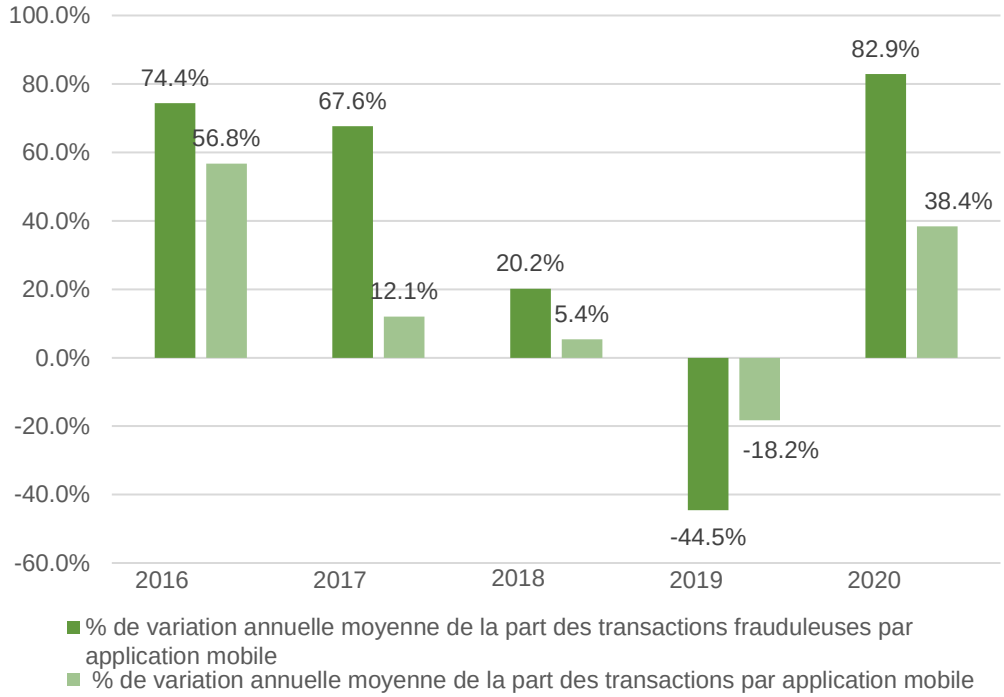
S.O. des informations et des données fiables ne sont pas disponibles ou suffisantes pour déterminer si le risque augmente ou baisse.

*Régions : Afrique, Asie de l'Est et Pacifique, Europe et Asie centrale, Amérique latine et Caraïbes, Moyen-Orient et Afrique du Nord, Asie du Sud.

**Dans certains pays, des éléments témoignent des améliorations à la suite de l'intervention du gouvernement (par exemple, la Chine et l'Inde).

LA FRAUDE PAR APPLICATION MOBILE* AUGMENTE PLUS RAPIDEMENT QUE L'UTILISATION D'APPLICATIONS MOBILES

Variation en pourcentage de la part des transactions frauduleuses par application mobile et de la part des transactions par application mobile (au niveau mondial)



Source : adapté du rapport de Outseer sur la fraude et les paiements, T2 2021, et de rapports trimestriels de RSA sur la fraude, T1 2018 et T3 2020.

Sur la base d'une recherche exploratoire utilisant des données d'applications mobiles à haute fréquence pour 71 pays, Fu et Mishra (2020) relèvent une augmentation de l'échelle et de la portée des applications mobiles financières frauduleuses et prédatrices ces dernières années, en particulier pendant la pandémie de COVID-19.

L'analyse des données des rapports trimestriels sur la fraude élaborés par Outseer** indique qu'entre 2016 et 2020, la part des transactions frauduleuses effectuées en utilisant des applications mobiles a progressé de 104 %, tandis que la part des transactions via des applications mobiles a crû de 34 %. Conformément à l'étude de Fu et Mishra, l'augmentation de la part des transactions frauduleuses et l'accroissement des transactions effectuées au moyen d'applications mobiles ont tous deux été plus prononcés pendant la pandémie de COVID-19. Entre 2019 et 2020, la part des transactions frauduleuses via des applications mobiles a enregistré une hausse de 83 %, tandis que la part des transactions via des applications mobiles a augmenté de 38 %.

Au troisième trimestre de 2020, les applications mobiles malveillantes sont devenues la principale source de fraude, dépassant l'hameçonnage qui était auparavant le vecteur d'attaque prédominant (Spajić 2021 ; RSA, 2018, 2020 ; Outseer 2021).

* RSA a défini la fraude sur application mobile comme étant « une activité basée sur une application mobile utilisant la marque d'une organisation sans autorisation ».
** Outseer est une nouvelle entreprise créée par RSA. La transition officielle des activités liées à la fraude et au renseignement de RSA a été annoncée officiellement le 9 juin 2021. Avant la création de la nouvelle entreprise, tous les rapports liés à la fraude étaient publiés par RSA.

LA FRAUDE PAR APPLICATION MOBILE AUGMENTE PLUS RAPIDEMENT QUE L'UTILISATION DE SMARTPHONES

Une analyse approfondie des applications de paiement mobiles Android de 246 prestataires de services de paiement mobile a révélé que certaines applications bancaires Android sans succursale font courir plus de risques aux utilisateurs que les systèmes existants (Reaves et al. 2015).

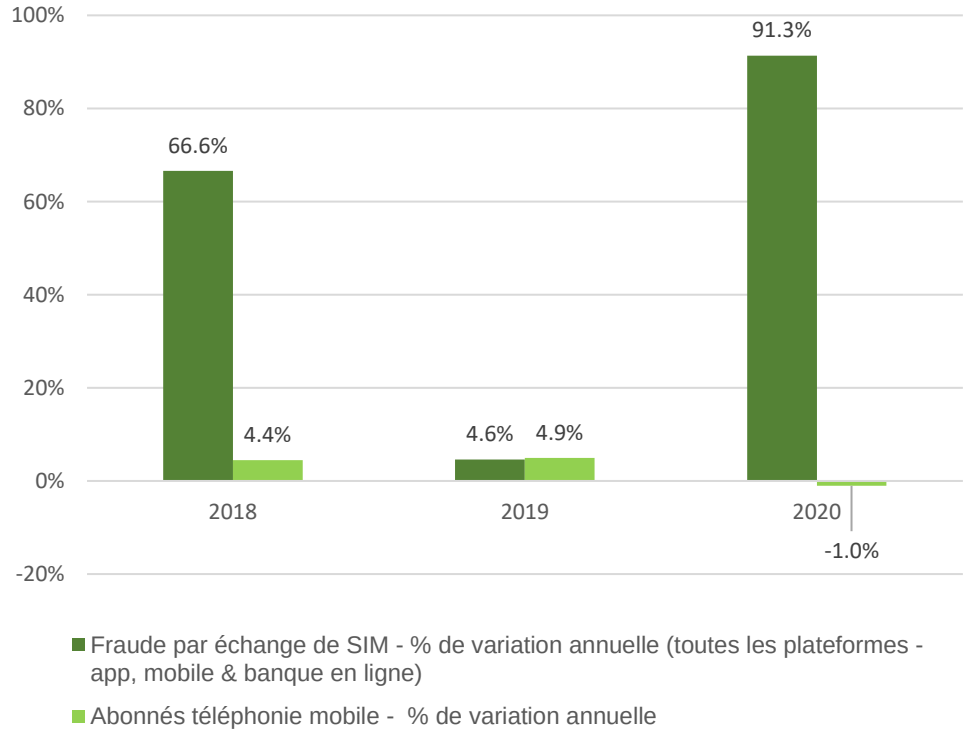
Les incidents de fraude par application mobile dans le secteur bancaire sud-africain ont augmenté de plus de 90 % entre 2017 et 2018, alors que le nombre d'utilisateurs de smartphones a augmenté de 10,3 % (Accenture 2020 ; SABRIC 2018 ; Statista 2021).

En Inde et au Kenya, des rapports indiquent que des applications de prêt frauduleuses et prédatrices ont exposé les clients du crédit numérique à des prêteurs abusifs (Duflos et al. 2021 ; Mukharji 2021 ; Palepu 2021 ; Singh 2021a, 2021b ; Faux 2020).

Photo pour ler CGAP par Saiyna Bashir via Communication for Development Ltd.

SELON CERTAINES DONNÉES EMPIRIQUES, LA FRAUDE PAR ÉCHANGE DE CARTES SIM AUGMENTE PLUS RAPIDEMENT QUE L'ADOPTION DE LA TÉLÉPHONIE MOBILE.

Variation en pourcentage des incidents liés à la fraude par échange de cartes SIM dans le secteur bancaire d'Afrique du Sud et chez les abonnés à la téléphonie mobile en Afrique du Sud 2018-2020



Source : Statistiques annuelles 2018, 2019, et 2020 (fraude par échange de cartes SIM) de la South African Banking and Risk Information Centre (SABRIC) ; Outil DataBank de la Banque mondiale (abonnés à la téléphonie mobile).

Le remplacement de la carte SIM est un service légitime proposé par les opérateurs de réseaux mobiles, qui permet aux clients de transférer les données de leur téléphone mobile d'un appareil à un autre lorsqu'ils changent d'appareil ou de prestataires de services. La fraude liée à l'échange de cartes SIM se produit lorsqu'un escroc lance une demande de portage et prend le contrôle du compte mobile d'un client, y compris les services liés au compte tels que l'argent mobile ou la banque mobile. Cependant, la plupart des pays ne publient pas de statistiques sur la fraude par échange de cartes SIM et les chiffres publiés sont parfois peu fiables (Priezkalns 2021).

> **« Même si la fraude par échange de cartes SIM est un phénomène mondial, elle est plus fréquemment observée dans les pays en développement.**
>
> –Farooq (2019)

Entre 2017 et 2020, les incidents de fraude par échange de cartes SIM en Afrique du Sud ont augmenté de 233 %, alors que le nombre d'abonnés à la téléphonie mobile a progressé de 8,4 % (rapports annuels SABRIC, 2018 et 2020 ; Outil DataBank de la Banque mondiale). En termes de pourcentage annuel, deux des trois années analysées ont enregistré une augmentation des incidents de fraude par échange de carte SIM plus importante que l'évolution du nombre d'abonnés à la téléphonie mobile. Parmi les trois canaux de fraude par échange de SIM, le mobile (c'est-à-dire via USSD) – souvent utilisé par les personnes à faible revenu – a représenté plus de 90 % des incidents de fraude par échange de cartes SIM en 2018 et 2019 et 88 % en 2020 de tous les incidents de fraude bancaire numérique en Afrique du Sud.

Des fraudes par échange de cartes SIM ont été signalées dans d'autres pays, comme au Mozambique, où la plus grande banque a enregistré une moyenne mensuelle de 17,2 cas d'échange de cartes SIM, et au Brésil, où 5 000 personnes ont été victimes d'une bande organisée spécialisée dans l'échange de cartes SIM (Assolini et Tenreiro 2019).

L'ESSOR DES PYRAMIDES DE PONZI NUMÉRIQUES POURRAIT COMPROMETTRE L'EXISTENCE DE VÉRITABLES SYSTÈMES D'INVESTISSEMENT

L'une des pyramides de Ponzi les plus marquantes qui a sévi au cours des dix dernières années est Ezubao, un système chinois de prêts de personne à personne qui s'est effondré en 2015 après avoir collecté plus de 9 milliards de dollars auprès de plus de 900 000 investisseurs. Une étude récente menée par Cheng et al. (2021) montre que l'effondrement d'Ezubao a eu une incidence indirecte sur d'autres sociétés légales de prêts P2P.

Impact du système P2P Ezubao (Cheng et al. 2021) 2021)

Effets indirects

- Le choc exogène subi par Renrendai, une société de prêts P2P légale..
- La réduction des montants des prêts alors que les taux d'intérêt augmentent..
- Tous les acteurs (les prêteurs, les emprunteurs et l'entreprise) ont été touchés.

Le nombre de pyramides de Ponzi numériques ne cesse d'augmenter (UIT, 2020). À preuve, dans les pays en développement et émergents, de nouveaux systèmes d'arnaque commencent à prospérer grâce à la cryptomonnaie.Les initiateurs de ces systèmes prétendent faire partie de réseaux d'entraide en calquant leurs systèmes sur le modèle des groupes d'épargne informels et des banques villageoises auxquels les acteurs de ces pays sont habitués. Les gestionnaires de fonds convainquent les consommateurs qui ne savent pas comment fonctionnent les plateformes de cryptomonnaies de leur confier leurs fonds afin qu'ils investissent en leur nom dans des cryptoactifs.

MMM, un système originaire de Russie, est un autre exemple. Le système s'est effondré en 1994 avant de refaire surface en 2011 avec un rayon d'action couvrant 80 pays. Le système MMM ciblait principalement les pays en développement et émergents tels que la Colombie, le Ghana, l'Inde, l'Indonésie, le Nigeria et le Zimbabwe (Solli 2019 ; Boshmaf et al. 2019 ; Chalwe-Mulenga et Duflos 2021). Parmi les stratagèmes utilisés, on peut citer : le hack de la société sud-africaine Africrypt, qui a permis d'arnaquer près de 3,6 milliards de dollars ; Mirror Trading International (MTI), une autre pyramide de Ponzi d'origine sud-africaine, qui a permis à ses initiateurs de détourner 588 millions de dollars et qui a touché plus de 260 000 investisseurs dans le monde ; et Dunamiscoin Resources, un système apparu en Ouganda qui a été démantelé en 2019 après avoir collecté 2,7 millions de dollars auprès de 4 000 investisseurs (Mureithi 2021 ; Henderson et Prinsloo 2021).

D'AUTRES TYPES DE FRAUDE ONT AUSSI GAGNÉ EN VOLUME ET EN TAILLE, NOTAMMENT PENDANT LA PANDÉMIE DE COVID-19

Tendances régionales en matière de fraude entre 2015 et 2018

Type de fraude	Amériques	Europe, Moyen-Orient et Afrique	Asie-Pacifique
Arnaques au paiement par autorisation*	↑ Hausse	↑ Hausse	↑ Hausse
Fraude en l'absence de carte physique	↑ Hausse	↑ Hausse	↑ Hausse
Vol d'identité/usurpation d'identité/prise de contrôle de compte	↑ Hausse	↑ Hausse	↑ Hausse

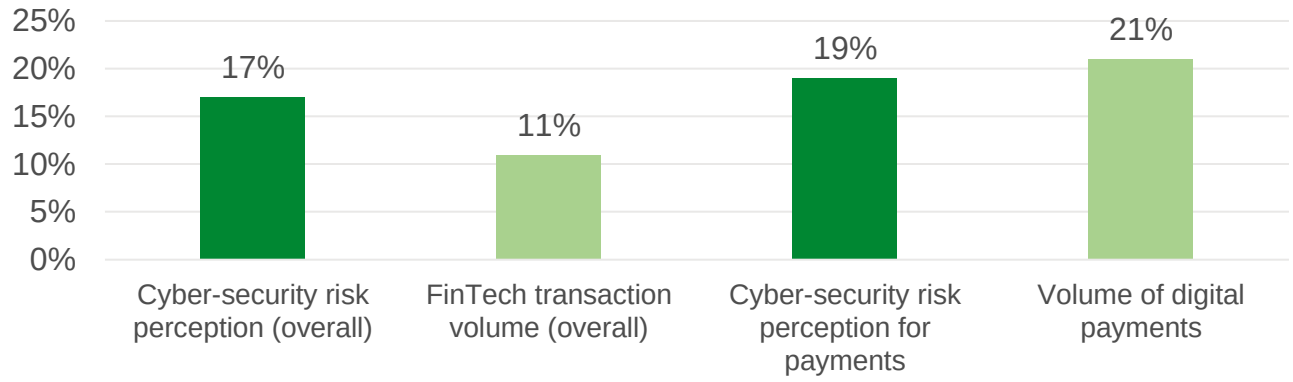
Source : : enquête mondiale de KPMG sur la fraude bancaire, menée auprès de 43 banques de détail entre novembre 2018 et février 2019.

*Les arnaques au paiement par autorisation se produisent lorsqu'un client est contraint de transférer son argent vers un compte contrôlé par le fraudeur en pensant que celui-ci est un bénéficiaire légitime.
Source : KPMG Global Banking Fraud Survey.

L'enquête mondiale de KPMG sur la fraude bancaire (2019b) relève que plus de la moitié des personnes interrogées ont fait état d'une augmentation des cas de fraude externe tels que les arnaques au paiement par autorisation, les fraudes lors de transactions sans cartes et l'usurpation d'identité.

L'enquête d'évaluation rapide du marché mondial réalisée par Fintech pour l'après-COVID-19 indique que, pour tous les produits étudiés, la perception du risque de cybersécurité s'est accrue à un rythme plus élevé que les volumes de transactions (sauf pour les paiements). Il ressort en outre de cette étude que la perception du risque de cybersécurité était plus forte dans les pays émergents et en développement (21 %) que dans les pays avancés (16 %).

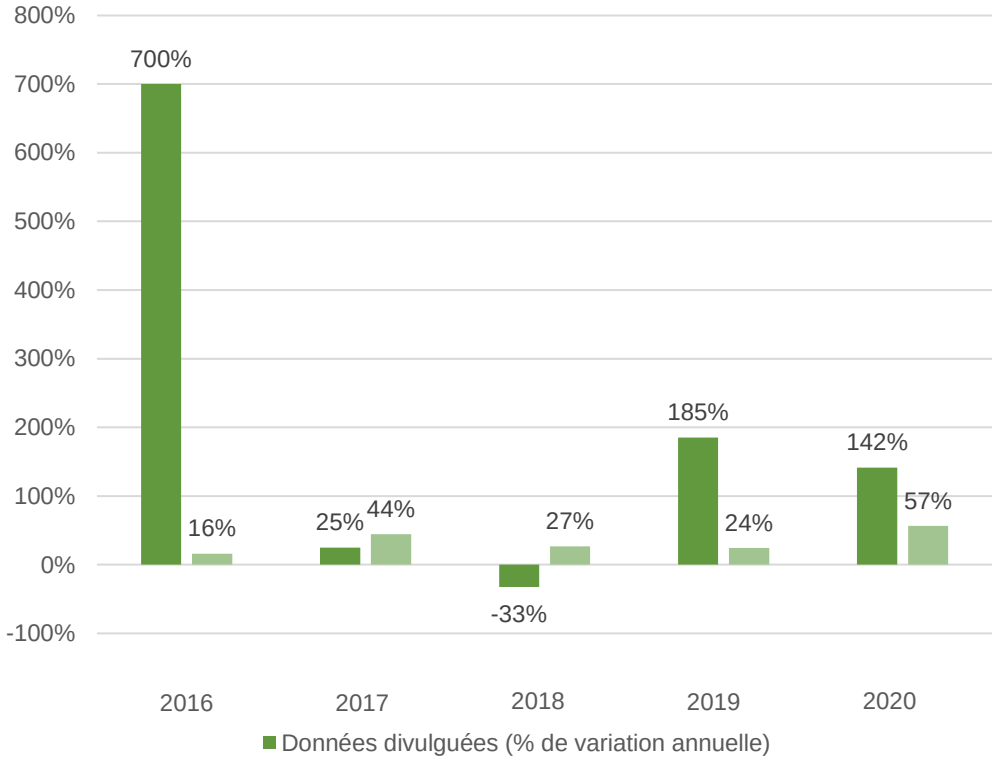
Croissance du secteur des technologies financières par rapport à la perception du risque cybernétique, variation en pourcentage en glissement annuel : juillet 2019–juillet 2020."



Source : Cambridge Center for Alternative Finance, Groupe de la Banque mondiale, et WEF, 2020, The Global COVID-19 FinTech Market Rapid Assessment Study, une enquête menée auprès de 1 385 entreprises de technologies financières opérant dans 169 juridictions.

L'AUGMENTATION DES INCIDENTS LIÉS AUX VIOLATIONS DE DONNÉES EST SUPÉRIEURE À L'AUGMENTATION DES DONNÉES CRÉÉES

Données mondiales créées et cas de violation de données, variations annuelles en pourcentage (2016-2020)



Source : données adaptées du rapport de fin d'année 2020 de Risk Based Security (nombre de cas de violation de données dans le monde) et de Statista (données mondiales créées).

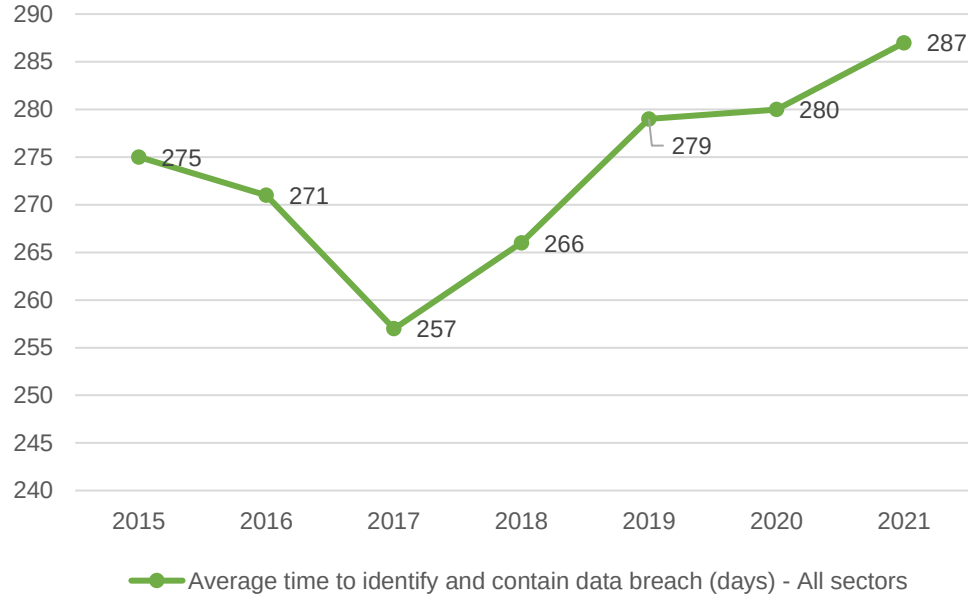
Entre 2015 et 2020 (exception faite de 2016, une année atypique), l'augmentation annuelle moyenne du nombre de cas de violation de données dans le monde était de 80 % et l'augmentation annuelle du volume de données créées était de 38 % (Risk Based Security 2020). Le nombre de cas de violation de données est passé de 0,8 milliard en 2015 à 37,2 milliards en 2020, ce qui constitue le record absolu dans l'histoire du rapport établi par Risk Based Security. Au cours de la même période, le volume des données créées dans le monde a augmenté, passant de 15,5 zettaoctets à 64,2 zettaoctets (Statista 2021). Entre 2016 et 2020, on a enregistré une progression annuelle en pourcentage du nombre de cas de violation de données plus importante que celle du nombre de données créées pendant trois années sur cinq (voir aussi Chalwe-Mulenga et Duflos, 2021). Il convient de relever que le score de gravité* s'est accru de manière constante tout au long de l'année 2020 pour atteindre une moyenne de 5,71 au quatrième trimestre, contre 4,75 au premier trimestre.

Il ressort de l'étude « Consumer Loss Barometer » menée par KPMG (2019a), qui mesure les perceptions des consommateurs en matière de cybersécurité, que les consommateurs des Amériques (43 %) ont signalé le niveau le plus élevé de compromission de fuites de données.Viennent ensuite les consommateurs de l'Asie-Pacifique (39 %), puis ceux de l'Europe, du Moyen-Orient et de l'Afrique (35 %). Il importe de souligner que les violations de données ont été classées parmi les principaux risques auxquels les utilisateurs des systèmes bancaires ouverts émergents sont exposés (Carr et al. 2018 ; Korobov 2020).

* Mesurée sur une échelle comprise entre 0 et 10, la gravité de la violation est dérivée du nombre de dossiers perdus, de la manière dont l'incident s'est produit, du type de données exposées et d'une série d'autres facteurs.

LES ORGANISATIONS PRENNENT PLUS DE TEMPS POUR DÉCELER ET NEUTRALISER UNE VIOLATION DE DONNÉES

Temps moyen nécessaire pour déceler et neutraliser une violation de données, 2015-2021



Source : adapté des rapports mondiaux d'IBM sur le coût d'une violation de données (2016-2021).

Même si les consommateurs peuvent ne pas se rendre compte que leurs données personnelles ont été piratées, une violation de données peut avoir des conséquences désastreuses sur eux.

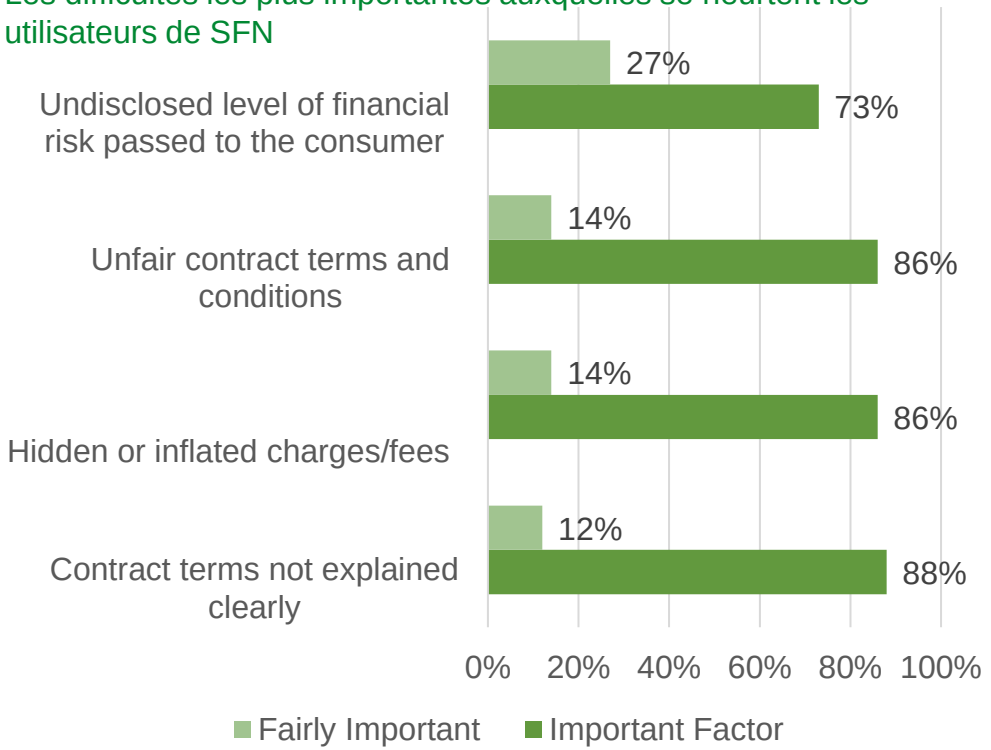
Le temps moyen pour déceler et neutraliser une violation de données est passé de 257 jours en 2017 à 287 jours en 2021 à cause de la sophistication accrue des cyberattaques qui exposent les données à caractère personnel des clients à des fuites.

IBM (2020) relève que les secteurs de la finance et de la santé ont connu les cycles de violation de données les plus longs : 233 jours et 326 jours, respectivement. Étant donné que le temps moyen nécessaire pour déceler et circonscrire une violation de données est lié au coût total de la violation, le coût moyen d'une violation de données devrait augmenter au cours des années à venir.

IBM (2021) souligne que pour les entreprises opérant dans des secteurs où les réglementations sont plus strictes (par exemple, le secteur financier), les coûts sont plus élevés au cours des années qui suivent une violation.

DES DONNÉES EMPIRIQUES MONTRENT QUE LA TRANSPARENCE A GLOBALEMENT DIMINUÉ

Les difficultés les plus importantes auxquelles se heurtent les utilisateurs de SFN



Source : adapté de l'enquête de Consumers International intitulée The Role of Consumer Organisations to Support Consumers of Financial Services in Low- and Middle-Income Countries et réalisée en 2020.

Une enquête mondiale menée auprès de 36 membres de Consumers International originaires de 32 pays à revenu faible ou intermédiaire a révélé que les quatre principaux défis auxquels les consommateurs de SFN étaient confrontés en 2020 tenaient au manque de transparence (Consumers International 2021).

Dans le segment du crédit numérique, les données disponibles semblent indiquer une corrélation entre le manque de transparence et le défaut de paiement ou le retard dans le remboursement des prêts numériques (Izaguirre et al. 2018a ; 2018a ; Izaguirre et al. 2018b ; Kaffenberger et al. 2018). C'est donc dire que la diminution de la transparence peut être un catalyseur dans les pays où les consommateurs ont brillé par des niveaux accrus de défaut de paiement ou par des cas de remboursement tardif de créances. Des pays tels que le Kenya, l'Inde, l'Indonésie et les Philippines par exemple ont enregistré dans un passé récent des niveaux plus élevés d'impayés chez les utilisateurs d'applications mobiles et de prêts P2P en partie faute d'avoir compris les taux et autres modalités des prêts contractés (Faux 2020 ; Singh 2021a ; Singh 2021b ; Prakarsa 2020 ; CNN Philippines 2021). L'aggravation des problèmes de transparence peut également être due à la complexité accrue des interfaces utilisateur, étant entendu qu'un nombre plus important de personnes dénuées de compétences numériques et financières utilisent désormais des smartphones (recherche Next Billion Users de Google).

Des améliorations en matière de transparence ont toutefois été constatées au Kenya après l'introduction d'une réglementation qui oblige les prestataires de services financiers mobiles à indiquer les prix sur les téléphones mobiles, comme en témoigne l'augmentation du nombre de clients qui connaissent désormais le coût de l'argent mobile (Mazer 2018).

LES VOIES DE RECOURS FORMELLES NE SONT PAS CONNUES OU COÛTENT CHER, MAIS LES DONNÉES SONT LIMITÉES POUR CONFIRMER CETTE HYPOTHÈSE

Les données et les bases factuelles mondiales et régionales sur l'évolution des risques relatifs à l'inadéquation des mécanismes de recours sont limitées.

Selon une étude qualitative menée auprès de consommateurs au Bangladesh, en Colombie et en Ouganda, seuls 11 % des clients en moyenne ayant rencontré des difficultés avec l'argent mobile l'ont signalé en ayant recours à un canal de réclamation formel tel qu'un centre de service client (McKee et al. 2015).

En Tanzanie et au Kenya, seuls 5 % et 10 % des emprunteurs numériques, respectivement, ont déjà contacté le service clientèle de leur prestataire de services financiers pour poser une question, exprimer une inquiétude ou porter une réclamation en rapport avec un prêt numérique (Kaffenberger et al. 2018).

Au Cambodge, une enquête menée auprès des clients pour recueillir leurs avis en ce qui concerne la protection des consommateurs a révélé que nombre d'usagers ignorent comment accéder aux mécanismes de traitement des plaintes de leurs prestataires de services financiers, et certains sont d'ailleurs peu enclins à avoir recours à un tel mécanisme même si le processus est clair (Kumari 2020).

Une étude menée en Indonésie a révélé que les centres d'appels représentaient le canal le plus coûteux pour la résolution des litiges. Pour la majorité des consommateurs (82 %), les agents constituent le principal canal de réclamation. De plus, 84 % des utilisateurs préfèrent engager des frais auprès des agents pour la résolution des litiges, contre 57 % qui contactent les centres d'appels (Mohammad et Pelupessy 2017).

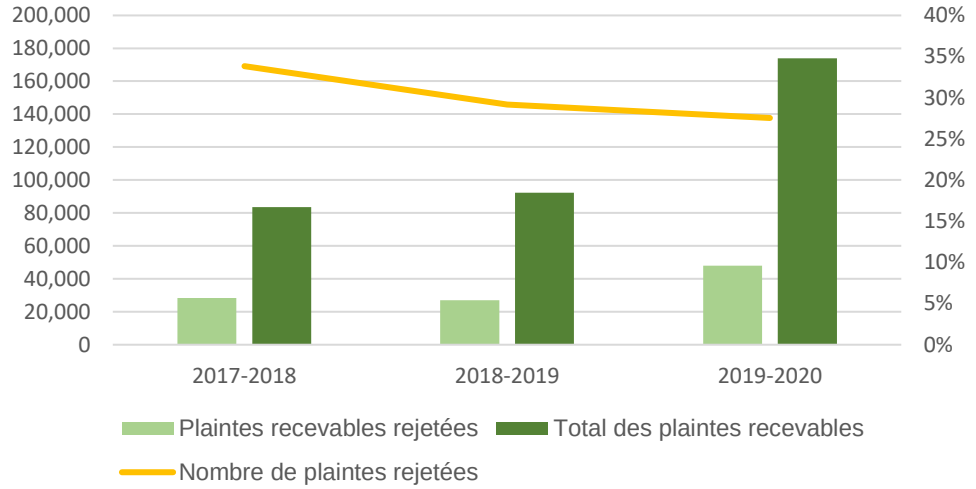
Il ressort de l'enquête sur l'usurpation d'identité et la fraude dans le monde menée par Experian dans 10 pays en 2021 que 50 % des entreprises interrogées ont accru leur dispositif d'accompagnement des clients en 2020. Or seulement 25 % environ des consommateurs ont indiqué recevoir des réponses plus rapides de la part du service client et ont pu contacter le service client s'ils étaient bloqués en ligne.

LE RECOURS EST UN PROCESSUS COMPLEXE ET TRACASSIER POUR LES CONSOMMATEURS

C'est notamment le cas en Inde

En Inde, la proportion de plaintes liées à des transactions numériques (notamment les transactions concernant les services bancaires mobiles ou de banque en ligne, les GAB/cartes de débit, ou encore les cartes de crédit) signalées au médiateur du secteur bancaire est passée de 33 % du nombre total des plaintes (soit 64 607 plaintes) en 2018-2019 à 45 % du total (137 823 plaintes) en 2019-2020, soit la plus grande proportion du nombre de plaintes.

Analyse des plaintes recevables concernant des transactions numériques rejetées par le médiateur du secteur bancaire indien



Source : : compilé par les auteurs sur la base d'informations tirées des documents suivants de la RBI : 2020 Banking Ombudsman Scheme, 2006, Ombudsman Scheme for NBFCs, 2018, et Ombudsman Scheme for Digital Transactions, 2019 : Rapport annuel – 1er juillet 2019 au 30 juin 2020.

Entre février 2019 et juin 2020, en tout 2 951 plaintes ont été signalées au programme de médiation concernant les transactions numériques (OSDT), un nouveau dispositif de régulation du secteur bancaire mis en place en 2019 pour traiter les plaintes liées aux services numériques introduites par les clients des participants au système non bancaire, sous l'égide de la Reserve Bank of India (RBI).

Une analyse des plaintes recevables* indique qu'entre 2017-2018 et 2019-2020, le nombre total de plaintes recevables et le nombre total de plaintes recevables rejetées se sont accrus. Cependant, le taux de rejet a diminué, passant de 34 % à 28 %, ce qui porte à croire que la qualité des plaintes s'est améliorée. On peut attribuer la légère amélioration de la qualité des plaintes aux programmes de sensibilisation institués par la RBI.

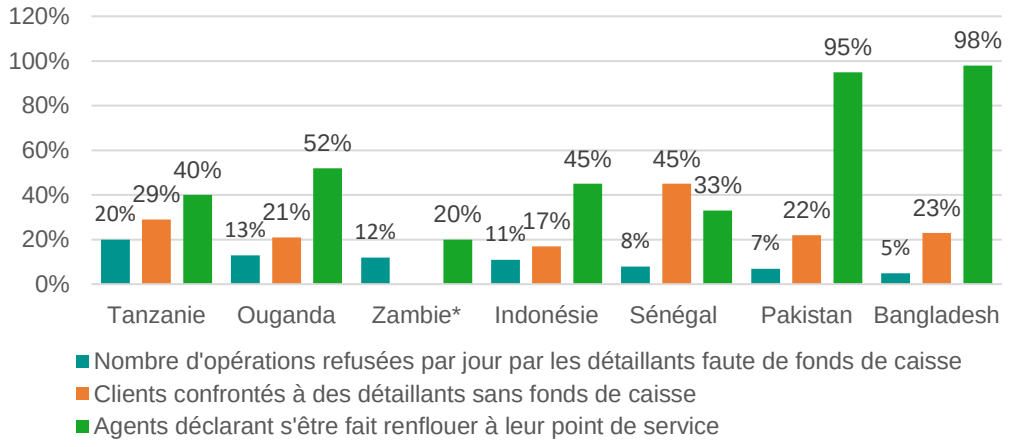
Néanmoins, en 2019-2020, en tout 72 % de toutes les plaintes reçues par les services du médiateur des banques provenaient des métropoles et des centres urbains, alors que les zones rurales et périurbaines représentaient 10 % et 18 %, respectivement, des plaintes déposées. Pas moins de 98 % des plaintes rejetées étaient dues à un dépôt sur des motifs peu clairs et au non-respect de la procédure, ce qui indique que les gens ne comprennent pas le système de dépôt des plaintes. Malgré quelques améliorations, les rapports indiquent que le système de recours est globalement complexe et tracassier en Inde, en particulier pour les personnes à faible revenu qui vivent en zone rurale et qui, en général, ignorent l'existence d'un médiateur du secteur bancaire. Cette complexité est aggravée par la modularisation du secteur financier (Sane 2021 ; Chivukula 2021).

* Les plaintes recevables sont celles qui sont adressées au médiateur du secteur bancaire, en rapport avec les motifs de plainte énumérés à l'article portant régime des services du médiateur du secteur bancaire – Banking Ombudsman Scheme (BOS), 2006 – et qui remplissent les conditions définies dans le programme. Les plaintes qui ne répondent pas aux normes établies sont rejetées.

L'INSUFFISANCE DES LIQUIDITÉS CHEZ LE DÉTAILLANT EMPÊCHE LES CONSOMMATEURS D'EFFECTUER DES TRANSACTIONS

Si de nouvelles solutions de gestion des liquidités chez le détaillant – telles que les « super-agents », les facilités de découvert et les algorithmes prédictifs pour les détaillants (Rodriguez et al. 2019 ; Wright et Bersudskaya 2017) peuvent aider à accroître le volume des liquidités chez le détaillant –, l'on peut constater que l'insuffisance des liquidités chez le détaillant reste un problème persistant dans certains pays (Genga et al. 2018 ; Kiarie et al. 2018; Unnikrishnan et al. 2019; Unnikrishnan et al. 2020).

Les clients face aux problèmes de liquidités des détaillants



Source : Genga et al. 2018 et Kiarie et al. 2018, sur la base des données des enquêtes menées par l'Agent Network Assessment.

* Les données relatives aux clients ayant rencontré des agents sans fonds de caisse n'étaient pas disponibles (Zambie).

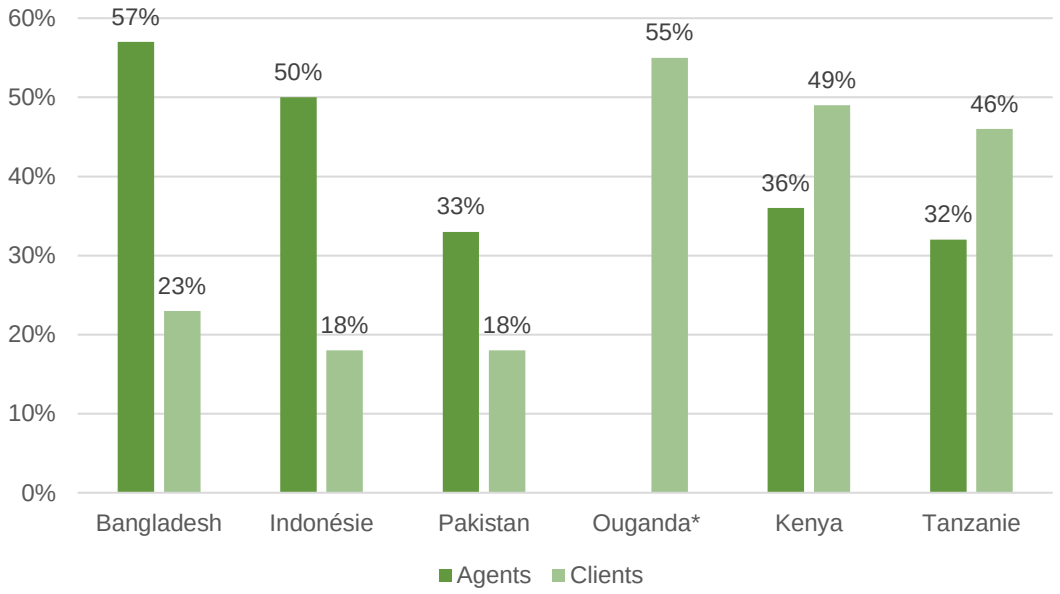
Cette situation est fréquente lorsque les agents se trouvent dans des localités éloignées des succursales du fournisseur de SFN. En Zambie, le manque de liquidités chez les détaillants a été mentionné comme un problème récurrent et critique qui déteint sur l'extension des activités des détaillants dans les zones rurales et difficiles d'accès (Holly et al., 2020 ; Harihareswara et al. 2019).

Les données factuelles du côté de l'offre établissent que certains pays ont enregistré des améliorations dans la gestion des liquidités chez le détaillant. En Inde, la proportion de détaillants qui se sont fait livrer des liquidités (toujours/parfois) s'est accrue, passant de 6 % en 2015 à 22 % en 2017. Sur cette même période, le nombre de détaillants qui se sont déplacés (parfois/toujours) afin de rééquilibrer le flottant a baissé, passant de 94 % à 81 % (Mehrotra et al. 2018).

Cependant, compte tenu de la rareté des données du côté de la demande, il est difficile d'établir si l'amélioration de la gestion des liquidités signalée par les détaillants a bénéficié aux consommateurs. Par exemple, 48 % des clients indiens vivant dans des centres urbains et 36 % des utilisateurs vivant en zone rurale ont déclaré que le manque de flottant ou de liquidités chez le détaillant posait problème lors de leurs transactions (CGAP et MSC, 2020). En outre, selon les données rapportées par Genga et al. (2018) comme par Kiarie et al. (2018), l'on constate que, dans tous les pays étudiés, la proportion des clients qui n'ont pas été capables d'effectuer leurs transactions faute de liquidités chez le détaillant était plus élevée que la proportion des transactions que des détaillants ont rejetées du fait d'un manque de liquidités.

LES PANNES DE RÉSEAU PEUVENT POUSSER LES CLIENTS À ADOPTER DES COMPORTEMENTS À RISQUE ET LEUR FAIRE PERDRE CONFIANCE DANS LE SECTEUR FINANCIER

Proportion de détaillants et de clients qui ont indiqué avoir été incapables d'aller au bout d'une transaction à cause d'une panne de réseau



Source : Genga et al. 2018, sur la base des données des enquêtes menées par l'Agent Network Assessment.

* Les données concernant les détaillants qui ont signalé des pannes de réseau n'étaient pas disponibles (Ouganda).

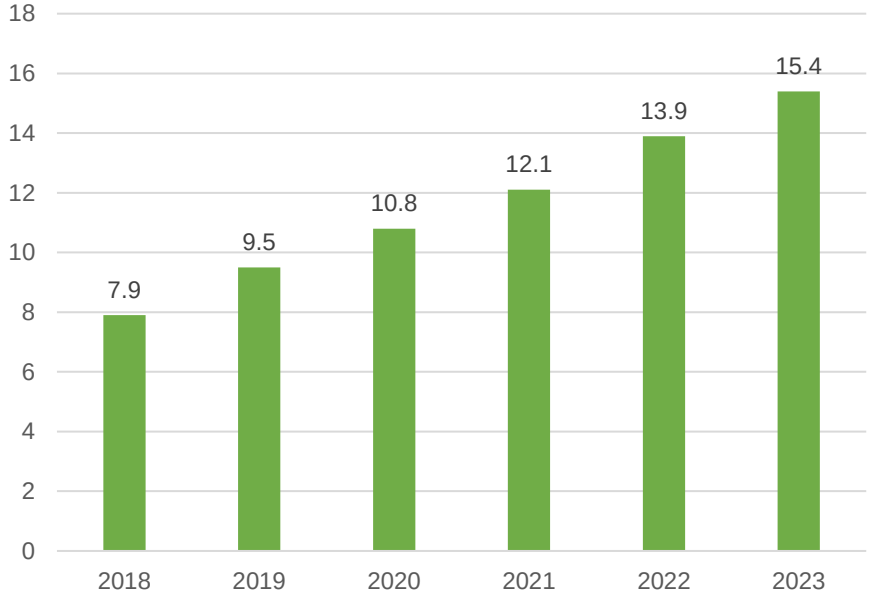
En 2015, les consommateurs de SFN ont cité les pannes de réseau comme une source de préoccupation majeure (McKee et al. 2015 ; Ahmed et Gomez 2015 ; Zimmerman et Baur-Yazbeck 2016). Bien que l'on ne dispose pas de données sur l'évolution des pannes de réseau dans les points de vente des détaillants, des éléments récents montrent que ces pannes de réseau sont devenues plus récurrentes dans le monde entier (cf. diapositive 30).

Les pannes de réseau donner lieu à des comportements à risque (par exemple un client qui laisse de l'argent, son code PIN ou son téléphone à un détaillant pour que celui-ci puisse effectuer la transaction lorsque le réseau est rétabli). Les pannes de réseau peuvent interrompre les activités quotidiennes des clients et entraîner une perte de confiance dans les services financiers formels.

En 2016, une interruption abrupte des services d'argent mobile qui s'est étendue sur quatre jours en Ouganda a privé des millions de personnes de l'accès aux fonds et aux services d'utilité publique tels que l'eau et l'électricité (Zimmerman et Baur-Yazbeck 2016).

LES ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ, UN RISQUE LIÉ AUX PANNES DE RÉSEAU, SONT PLUS NOMBREUSES ET PLUS RÉCURRENTES

Nombre d'attaques mondiales par déni de service distribué (en millions)



Source : rapport annuel sur l'Internet de Cisco (2020–2023)."

Voir l'annexe pour d'autres exemples de l'évolution des risques pour les consommateurs de services financiers numériques.

Les pannes de réseau constituent un vaste problème qui peut être attribué à des difficultés telles qu'une mauvaise infrastructure, des pannes de courant ou des attaques malveillantes comme les attaques par déni de service distribué. Une attaque par déni de service distribué se produit lorsque plusieurs systèmes inondent la bande passante ou les ressources d'un système ciblé. Cette situation peut se produire lorsque des pirates tentent d'inonder un réseau à l'aide de volumes anormalement élevés de trafic de données dans l'intention de le paralyser. Les estimations montrent que si la vitesse de la téléphonie cellulaire mobile va plus que tripler d'ici à 2023 pour atteindre 43,9 Mbits/s contre 13,2 Mbits/s en 2018, le nombre d'attaques par déni de service distribué passera du simple au double pour atteindre 15,4 millions d'attaques d'ici à 2023, contre 7,9 millions d'attaques en 2018 (Cisco 2020).

Le rapport annuel de Cisco sur l'Internet (2020-2023) indique qu'entre 2018 et 2019, la fréquence mondiale des attaques par déni de service distribué a augmenté de 39 %, tandis que les attaques entre 100 Gbits/s et 400 Gbits/s ont augmenté de 776 %. Sur la même période, la taille moyenne des attaques par déni de service distribué était de 1 Gbits/s, ce qui est suffisant pour mettre la plupart des organisations complètement hors ligne.

En 2020, une faille de sécurité sur un agrégateur de crédit à la consommation, affectant principalement les transferts de la banque vers un portefeuille mobile, a occasionné une suspension indéfinie des transactions d'argent mobile par le plus grand fournisseur d'argent mobile en Ouganda (Kafeero 2020).

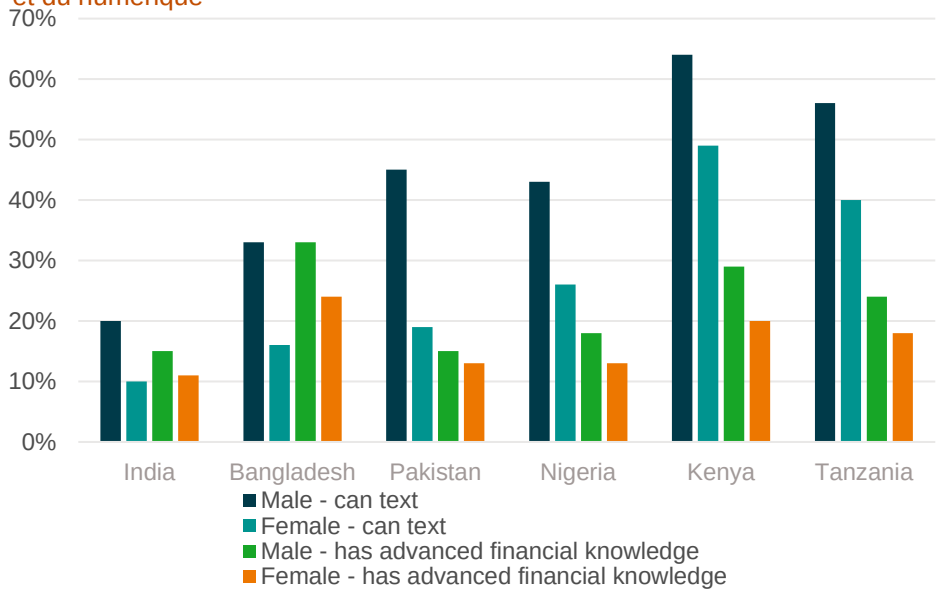
IV. RISQUES INHÉRENTS AUX SERVICES FINANCIERS NUMÉRIQUES (SFN) ET VULNÉRABITÉ DES CONSOMMATEURS

VULNÉRABILITÉ ACCRUE DES FEMMES À FAIBLE REVENU AUX RISQUES INHÉRENTS AUX SERVICES FINANCIERS NUMÉRIQUES

Les faibles compétences dans les domaines de l'écriture et de la lecture, du numérique et de la finance exposent davantage les femmes aux risques que présentent les services financiers numériques (SFN).

Les données ventilées disponibles permettant d'évaluer l'évolution des risques que présentent les SFN pour les femmes restent limitées. Certaines observations anecdotiques indiquent que ces dernières sont plus exposées que les hommes à ces risques.

Aptitudes des hommes et des femmes du milieu rural dans les domaines de la finance et du numérique



Source : IDEO.org et la Fondation Bill & Melinda, 2019, Women and Money:IDEO.org et la Fondation Bill & Melinda, 2019, Women and Money: Insights and a Path to Close the Gender Gap.Insights and a Path to Close the Gender Gap.

Cette situation s'explique notamment par les plus faibles capacités d'écriture et de lecture des femmes, ainsi que leur moins bonne connaissance du numérique et de la finance (GPFI 2020 ; GSMA 2020 ; Toronto Centre 2018 ; Wechsler et Siwakoti 2020). Les parties prenantes qui œuvrent à l'inclusion financière et à la protection des consommateurs doivent recueillir davantage d'informations ventilées par genre. Lorsque des femmes, qui ont des aptitudes limitées dans les domaines de la finance et du numérique, ont la possibilité d'utiliser des SFN, elles s'exposent à différents risques dès lors qu'elles ne comprennent pas nécessairement les conditions et/ou les tarifications associées à ces services. Elles sont souvent victimes de fraudes.

En Indonésie, après la numérisation du Program Keluarga Harapan (PKH) – un programme de paiement « gouvernement à personne » (G2P) qui a bénéficié à quelque 10 millions de consommateurs –, un sondage a montré que près de la moitié (44 %) des femmes interrogées demandaient de l'aide au personnel de sécurité à proximité des guichets automatiques (GAB), aux agents des établissements bancaires ou à leurs proches pour effectuer des retraits. En outre, de nombreuses femmes ont indiqué qu'elles préféraient s'adresser à un agent plutôt que d'utiliser un GAB, car le préposé se chargeait de la totalité de l'opération à leur place.

Certaines études montrent également que les femmes ne changent pas nécessairement leur code PIN par défaut et utilisent même parfois le même que des personnes de leur entourage pour éviter les erreurs autant que possible. Il leur arrive même de tendre leur téléphone à un agent pour que ce dernier procède à la transaction (Theis et al. 2020 ; IDEO.org et la Fondation Bill & Melinda Gates 2019 ; Wright et al.2020 ; IDEO.org et la Fondation Bill & Melinda Gates 2019 ; Wright et al. 2018).

EXEMPLES DES RISQUES QUE PRÉSENTENT LES SFN POUR LES FEMMES À FAIBLE REVENU

Les SFN présentent plusieurs risques pour les femmes à faible revenu, mais les données disponibles sur l'évolution de ces risques sont limitées.

Quatre grands types de risques

FRAUDE

Exemple:
- Pyramide de Ponzi

D'après une étude menée en Chine, les femmes courent davantage de risques d'accuser des pertes dans une pyramide de Ponzi.

USAGE ABUSIF DES DONNÉES

Exemple:
- Biais algorithmique

Compte tenu des données biaisées, les femmes sont plus susceptibles

d'être victimes de discrimination algorithmique.

MANQUE DE TRANSPARENCE

Exemple:
- Complexité de l'interface utilisateur

Davantage de femmes ont accès à des smartphones, mais elles sont moins nombreuses à avoir les compétences numériques requises pour comprendre les termes des contrats et les informations de tarification.

INADÉQUATION DES MÉCANISMES DE RECOURS

Exemple:
- Normes sociales/agents femmes moins nombreuses

Par exemple, les femmes peuvent ne pas se plaindre d'un problème lié aux SFN lorsqu'elles tombent sur un agent de sexe opposé.

Deux types de risques transversaux

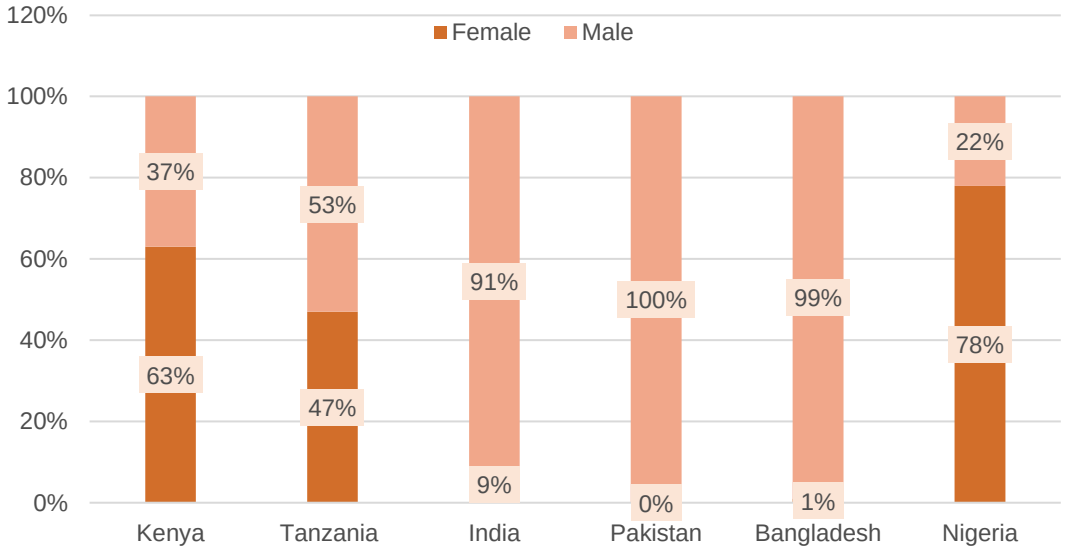
RISQUES LIÉS AUX AGENTS
Fraude imputable à l'agent – Par exemple, les femmes sont plus vite la cible d'agissements préjudiciables, d'après certaines données recueillies au Ghana.

PANNE DE RÉSEAU
Compte tenu de leurs compétences numériques et capacités de lecture et d'écriture plus faibles, les femmes sont davantage susceptibles d'adopter des comportements à risque comme, par exemple, passer leur téléphone à d'autres personnes, y compris des agents, lorsque le réseau est en panne.

LES NORMES SOCIALES ET LES AGISSEMENTS PRÉJUDICIABLES DES AGENTS REPRÉSENTENT UN DÉFI POUR LES FEMMES

Les femmes préfèrent s'adresser à des agents femmes, qui sont malheureusement moins nombreuses et plus enclines à surfacturer.

Proportion d'agents femmes et d'agents hommes



Source : IDEO.org et la Fondation Bill & Melinda, 2019, Women and Money :IDEO.org et la Fondation Bill & Melinda, 2019, Women and Money : Insights and a Path to Close the Gender Gap.Insights and a Path to Close the Gender Gap.

En République Démocratique du Congo, Chamboko et al. (2020) ont pu établir une « correspondance préférentielle des genres dans les transactions bancaires, les clientes et clients préférant avoir affaire à des agents de leur propre sexe ». Ils ont également constaté que les femmes préféraient s'adresser à des agents femmes, même moins disponibles, en particulier « lorsqu'elles effectuaient des transactions importantes ou que leur compte affichait un solde élevé ».

Au Bangladesh, la Société financière internationale (IFC) a établi que, en 2018, 52 % des femmes préféraient nettement avoir affaire à des agents femmes, mêmes si elles étaient conscientes qu'elles devraient s'adresser, dans 99 % des cas, à des agents hommes.

Les femmes préfèrent rester aux côtés des agents, une attitude jugée inconvenante dans la plupart des cultures, en particulier au Pakistan et au Bangladesh (IDEO.org et la Fondation Bill & Melinda Gates 2019 ; Kabir et Klugman 2019). Les agents femmes sont également considérées comme plus patientes et sont, de ce fait, de meilleurs éléments pour assurer un rôle pédagogique. Malheureusement la plupart des femmes n'aspirent pas à devenir agents.

Toutefois, certains indices troublants montrent, au Ghana, que les agents femmes sont plus enclines à des comportements relevant de l'« inconduite ». Dans une étude du marché du paiement mobile, au sein de 166 collectivités à faible revenu de la partie orientale du pays, Annan (2021) a trouvé des éléments attestant une « inconduite plus ou moins marquée selon le genre ». En règle générale, 25 % des opérations sur le marché du paiement mobile sont surfacturées et, bien que les agents des deux sexes appliquent des tarifs excessifs, les agents femmes ont davantage (37 %) recours à cette pratique, auprès des clients des deux sexes.

LES FEMMES SONT LA CIBLE D'OPÉRATIONS FRAUDULEUSES ET D'ABUS EN LIGNE

Selon certaines données anecdotiques, les femmes sont plus susceptibles d'être la cible d'intimidations en ligne et d'enregistrer des pertes plus élevées dans des pyramides de Ponzi.

Les femmes qui investissent dans des pyramides de Ponzi sont plus réceptives à l'affinité avec l'investisseur.

Une étude menée en Chine a tenté de déterminer dans quelle mesure l'affinité avec l'investisseur (au regard du genre et de l'âge) influait sur l'extension d'une pyramide de Ponzi et de quelle manière les investisseurs subissent des pertes. Elle a établi que les femmes investisseurs, qui rejoignaient une pyramide de Ponzi, sur les conseils d'autres femmes investisseurs, couraient davantage de risques d'enregistrer des pertes lorsque la pyramide – numérique ou pas – s'écroulait (Huang et al. 2021).

Selon certains reportages récents présentés par des journalistes argentins, une célébrité aurait malicieusement attiré plusieurs femmes dans un système de pyramide féministe, appelé « telares de abundancia » (« l'abondance à portée de main »). Vanté sur les médias sociaux et par des groupements solidaires sur Whatsapp, le système de pyramide s'est nourri de l'activisme des mouvements féministes, né de la détérioration du contexte économique et des injustices à l'encontre des femmes (Schwartz et Herrera 2020 ; Bleszynska 2021 ; Gibbings 2020 ; Fahsbender 2019). Par ailleurs, ces reportages indiquent que ces montages sont de plus en plus répandus dans d'autres pays d'Amérique latine.

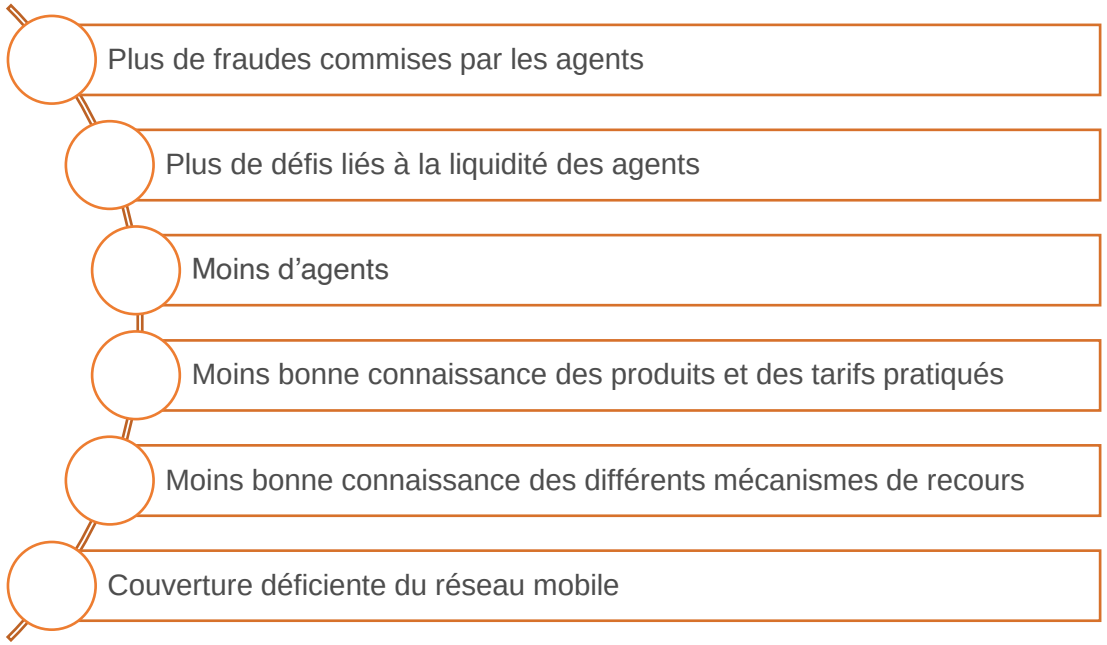
Les utilisatrices de SFN peuvent être dans l'obligation de fournir des « garanties dénudées ».

En 2016 et 2017, certains rapports publiés dans les médias chinois indiquaient que des étudiantes devaient fournir des photos d'elles, dénudées ou obscènes, comme garantie pour pouvoir obtenir un crédit numérique. Les prêteurs menaçaient alors de publier les photos sur les réseaux sociaux si les jeunes femmes ne remboursaient pas leurs dettes. Un organe de presse a trouvé un fichier de « garanties dénudées » dans lequel 160 jeunes filles, inscrites à l'université, montraient leur carte d'identité (Zhang and Woo 2017 ; Bradsher et Tang 2017). Ces activités ont été observées sur le marché non régulé du crédit numérique qui, à cette époque, était en plein essor en Chine. Il convient de mentionner que les femmes courent davantage de risques d'être victimes d'abus en ligne (Sambasivan et al. 2019).

Des mesures proactives doivent être adoptées pour éviter toute pratique agressive de recouvrement des dettes, en particulier sur les marchés où les crédits numériques, proposés via des applications, constituent une nouveauté.

VULNÉRABILITÉ ACCRUE DES POPULATIONS RURALES AUX SFN

À l'instar des femmes, les populations rurales ont peu de compétences dans les domaines de l'écriture et de la lecture, du numérique et de la finance ; de ce fait, elles sont davantage exposées aux risques inhérents aux SFN.



Compte tenu de l'utilisation peu répandue des SFN dans les zones rurales, les données relatives aux risques réels qu'encourent ces populations sont anecdotiques.

Contrairement aux zones urbaines, les zones rurales comptent moins d'agents et proposent un choix de SFN plus limité (Mustafa et al. 2017; Unnikrishnan et al. 2019). Par conséquent, peu de données tangibles existent sur l'échelle des risques que présentent les SFN pour le consommateur.

Les populations rurales qui utilisent les SFN courent des risques similaires, voire identiques dans certains cas, à ceux des femmes à faible revenu. Le danger est plus grand encore lorsque les consommateurs ruraux sont des femmes. Une étude menée dans les campagnes, en Indonésie, a permis d'établir qu'entre 15 et 40 % seulement des consommateurs étaient au fait des frais de transaction, et que cette ignorance permettait aux agents de surfacturer les services.

Elle a également montré que les consommateurs en milieu rural faisaient face à d'autres problèmes, comme l'inadéquation des mécanismes de recours, les ventes abusives, les retards et les refus de transaction (Mohammad et Pelupessy 2017). Selon une enquête menée en 2019 au Kenya par FinAccess, les consommateurs en milieu rural sont plus nombreux (42,2 %) à être tributaires de leurs connaissances de la finance que leurs pendants en ville (35,8 %).

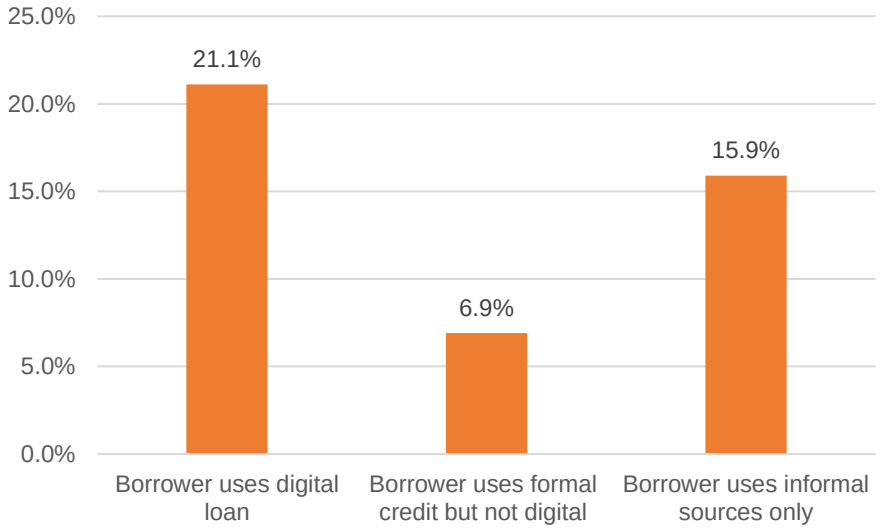
Dans certains pays, les problèmes de liquidité des agents sont plus importants en milieu rural (Harihareswara et al. 2019 ; White 2020 ; Kiarie et al. 2018).

V. ÉCLAIRAGE SPÉCIAL : SURENDETTEMENT DES SOUSCRIPTEURS DE CRÉDITS NUMÉRIQUES

LES PRÊTEURS NUMÉRIQUES SONT PLUS ENCLINS À PROMOUVOIR DES EMPRUNTS MALSAINS QUI ENTRAÎNENT DES TAUX DE NON-REMBOURSEMENT ÉLEVÉS

Les consommateurs courent davantage de risques de se retrouver en défaut de paiement s'ils utilisent une application bancaire.

Emprunteurs qui se sont retrouvés au moins une fois en situation de défaut de paiement pour un crédit au cours des douze derniers mois



Source : FSD Kenya, Digital Credit in Kenya : Facts and Figures from FinAccess, 2019.Facts and Figures from FinAccess, 2019.

* Un crédit cumulé désigne plusieurs encours de crédits simultanés, qui nuisent à la capacité de remboursement de l'emprunteur dans les délais impartis.* C'est également un indicateur de fraude à l'identité.

Un nombre croissant de consommateurs ont accès à des produits de crédit grâce à leurs applications mobiles ainsi qu'à des plates-formes de prêts entre pairs. Toutefois, ces différents circuits les exposent à de nombreux risques qui mènent au surendettement. Selon les données recueillies en 2019 par FinAccess, les emprunteurs numériques (21,1 %) courent davantage de risques de défaut de paiement que les emprunteurs informels (15,9 %) et les emprunteurs non numériques classiques (6,9 %). En outre, 14 % des emprunteurs numériques ont déclaré s'être spécifiquement retrouvés dans une situation d'insolvabilité après avoir contracté un prêt via un site bancaire en ligne ou une application numérique (FSD Kenya 2019).

Une étude visant à évaluer les progrès du crédit numérique ainsi que les défis liés à ce type de produits au Kenya a établi que la proportion de crédits numériques (91,2 % en 2018) avait non seulement augmenté, mais aussi largement dépassé celle des prêts traditionnels (8,8 % en 2018). Toutefois, près de 2,2 millions de personnes, qui avaient obtenu un crédit numérique entre 2006 et 2018, avaient des crédits improductifs et 49 % de ces emprunteurs numériques avaient des soldes restants dus inférieurs à 10 dollars.

Comme toutes les autres, cette étude a confirmé le manque de transparence alors que les clients comprenaient mal les questions de tarification ainsi que les modalités et conditions. En outre, les clients ne savaient pas comment leurs données personnelles étaient partagées.

LE SURENDETTEMENT EST LE RÉSULTAT D'UN FAISCEAU DE RISQUES INHÉRENTS AUX SFN POUR LE CONSOMMATEUR

Les consommateurs de crédits numériques surendettés sont confrontés à plusieurs risques.

Principaux risques qui contribuent au surendettement

FRAUDE

- Applications mobiles et plates-formes P2P non autorisées

USAGE ABUSIF DES DONNÉES

- Intrusion dans la vie privée
- Pratiques injustes (par ex. : intimidation en ligne)

MANQUE DE TRANSPARENCE

- Produits inadaptés
- Taux effectif global (APR) non communiqué

INADÉQUATION DES MÉCANISMES DE RECOURS

- Aucun système de recours disponible

Risques transversaux qui contribuent au surendettement

RISQUES LIÉS AUX AGENTS
Les agents appellent sans cesse les emprunteurs ; les agents prennent contact avec leurs proches et leurs amis.

PANNE DE RÉSEAU
Échec de la transaction (remboursement) lorsque le système est lent ou qu'il est hors service.

Retombées négatives

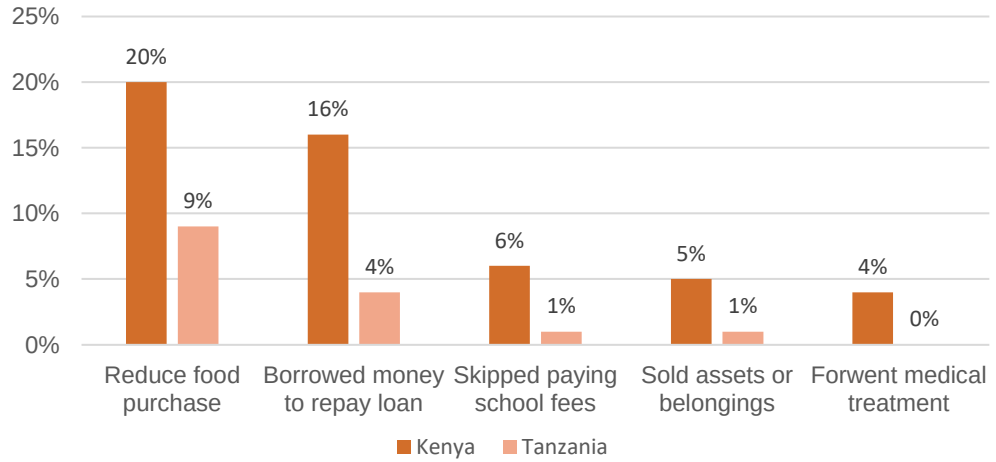
Les consommateurs s'endettent et commencent à accumuler les crédits (c'est-à-dire qu'ils souscrivent des emprunts multiples sur une courte période pour rembourser des crédits existants). Les consommateurs peuvent également sauter des repas, vendre des actifs ou ne plus s'acquitter des frais de scolarité de leurs enfants.

LE SURENDETTEMENT A DES EFFETS INQUIÉTANTS SUR LA VIE ET LES MOYENS DE SUBSISTANCE DES POPULATIONS

Il nuit à la capacité des consommateurs de résister aux chocs et conduit à la mise en place de mécanismes d'adaptation inadéquats.

Le surendettement peut conduire à des décisions préjudiciables, qui minent la capacité de résister aux chocs et de gérer le stress. En Tanzanie et au Kenya, une étude a montré que les consommateurs réduisaient leurs achats de denrées alimentaires et contractaient de nouveaux prêts pour rembourser une dette existante.

Mesures adoptées pour rembourser des crédits numériques au Kenya et en Tanzanie



Source : Kaffenberger,Totolo et Soursourian, 2018, A Digital Credit Revolution:Kaffenberger,Totolo et Soursourian, 2018, A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania.Insights from Borrowers in Kenya and Tanzania.

Une autre étude menée au Kenya a révélé que le recours au crédit numérique accroissait les probabilités qu'un ménage doive liquider certains actifs pour rembourser un emprunt, et doive également souscrire d'autres crédits, et ce, au préjudice de son bien-être (Wamalwa et al. 2019).

Les indicateurs de difficultés de remboursement des emprunteurs numériques (par ex. : la réduction des achats de denrées alimentaires, les emprunts excessifs, la déscolarisation d'un enfant) sont plus proches des indicateurs des emprunteurs informels que de ceux des emprunteurs formels (FSD Kenya 2019).

Selon des rapports de presse publiés en Chine, au Kenya et en Inde, certaines personnes surendettées, victimes d'intimidation en ligne, ont mis fin à leurs jours (Zhang et Woo 2017 ; Faux 2020 ; Mashal et Kumar 2021 ; Singh 2021a, 2021b).

Des données émanant de la Suède indiquent que les personnes surendettées ont neuf fois plus de chances de tomber malades et sept fois plus de sombrer dans la dépression que les personnes ne connaissant pas ce problème (Political Economy Research Centre 2015 ; Ferreira et al. 2021 ; Ahlström et Tjulander 2020).

VI. LA VOIE À SUIVRE : APPEL À L’ACTION

CONSÉQUENCES POUR LES ORGANISMES DE RÉGLEMENTATION ET DE SUPERVISION

Des mesures proactives s'imposent de toute urgence pour garder la confiance du consommateur en les SFN et lui assurer des retombées positives.

Si les SFN continuent de présenter des risques sans cesse croissants, les consommateurs vulnérables pourraient leur retirer leur confiance. **Les organismes de réglementation et de supervision** ont un rôle capital à jouer dans l'atténuation de ces risques.

Les organismes de réglementation et de supervision peuvent mettre en place des outils et des mesures permettant d'effectuer un suivi et d'intervenir au moment opportun en vue d'atténuer les risques que présentent les SFN et de minimiser le préjudice causé aux clients. Ils peuvent notamment :

- mettre en place des outils de suivi du marché afin de mieux évaluer la situation, dans les temps et en permanence, notamment celle des femmes et des pans vulnérables de la société ;
- instaurer des exigences réglementaires pour certains aspects particuliers comme, par exemple, la cybersécurité, la transparence ainsi que la gestion des données et des plaintes ;
- veiller à la stricte application des règles de supervision ;
- mettre au point des mécanismes permettant de collaborer avec les organismes de réglementation du secteur non financier (concurrence, télécommunications, autorités de protection des données ; organismes chargés de l'application des lois) ;
- réorienter l'inclusion financière sur les retombées positives en faveur du client plutôt que sur l'accès et l'utilisation ;
- pousser les autorités nationales à soutenir également les cadres juridiques de protection du consommateur.

Photo pour le CGAP de Lorena Velasco via Communication for Development Ltd.

CONSÉQUENCES POUR LES BAILLEURS DE FONDS ET LES INVESTISSEURS

Les bailleurs de fonds et les investisseurs peuvent contribuer à promouvoir des pratiques responsables au regard des SFN.

Les **bailleurs de fonds** peuvent examiner, dans la conception et les évaluations d'un projet de SFN, les risques que ce dernier peut présenter pour le consommateur. Ils peuvent également contribuer à la littératie financière et numérique des clients vulnérables, et leur permettre ainsi de prendre conscience des risques. Les bailleurs de fonds peuvent aussi promouvoir et soutenir :

- la coordination des organismes de réglementation des marchés de la finance, des données et des télécoms ;
- le dialogue entre les décideurs, les organismes de réglementation, les organismes de supervision, les prestataires de SFN et les associations de consommateurs ;
- les cadres de gouvernance ;
- l'infrastructure habilitante (par ex. : systèmes d'identification) ;
- le financement de la recherche sur les risques pour le consommateur.

Les investisseurs peuvent, au titre du devoir de vigilance, examiner les mécanismes de gestion des risques et les stratégies de protection du consommateur qui sont en place dans les sociétés détenues. Ils peuvent également promouvoir, chez les prestataires de SFN, l'adoption de normes de conduite responsable, par exemple en adhérant aux lignes directrices de l'investisseur sur les placements responsables dans des SFN. Ils peuvent par ailleurs inciter les sociétés détenues à aider les consommateurs à gagner en autonomie, par une meilleure littératie financière numérique.

Photo pour le CGAP de Lorena Velasco via Communication for Development Ltd.

CONSÉQUENCES POUR LES PRESTATAIRES DE SFN

Les prestataires de SFN ont un rôle capital à jouer puisqu'ils sont directement en contact avec les clients.

Pour aider les clients à cerner et à atténuer les risques, les prestataires de SFN sont encouragés à inclure la littératie financière dans leurs modèles commerciaux et à mettre en place, à l'échelle du secteur, des mécanismes visant à promouvoir les pratiques responsables en matière de SFN. Les prestataires peuvent également évaluer la solidité financière de leurs clients et élaborer des modèles commerciaux axés sur les consommateurs, qui permettent à ces derniers d'obtenir des résultats positifs (UNSGSA 2021 ; CGAP Customer-Centric Guide). En outre, ils peuvent renforcer leur cyberrésilience et y apporter des améliorations continues.

Ils peuvent notamment prendre des mesures supplémentaires pour améliorer :

- les protocoles de gestion des plaintes ;
- la conception des produits afin de minimiser les risques ;
- la transparence des produits ;
- la gestion des liquidités des agents ;
- la disponibilité des systèmes, par des mises à niveau fréquentes des systèmes de technologies de l'information (STI).

Photo de Chara Lata Sharma, concours de photographie CGAP

CONSÉQUENCES POUR LES ASSOCIATIONS DE CONSOMMATEURS ET LES CHERCHEURS

Les associations de consommateurs et les chercheurs ont également un rôle à jouer.

Les **associations de consommateurs** peuvent sensibiliser aux risques inhérents aux SFN et fournir des informations sur les stratégies d'atténuation. Elles peuvent également :

- aider les consommateurs en difficultés, en particulier les plus vulnérables, à introduire une plainte ;
- renseigner les consommateurs sur les risques ;
- apporter aux consommateurs une aide juridique ou autre ;
- proposer l'intervention de fonds d'indemnisation ;
- informer les organismes de supervision et de réglementation des préoccupations naissantes des consommateurs.

Les **chercheurs** peuvent continuer à combler les lacunes décelées dans ce travail comme, par exemple, le manque de données ventilées par genre et l'absence d'éléments probants sur les conséquences des risques sur le consommateur – en particulier les plus vulnérables.

Photo pour le CGAP de Nicolas Réméné via Communication for Development Ltd.

SOLUTIONS DU CGAP POUR PROTÉGER LES CLIENTS VULNÉRABLES

Le CGAP est favorable à une approche dans laquelle les organismes de réglementation, de supervision, les prestataires et les facilitateurs de marché s'efforcent avant tout d'assurer **aux clients le succès de leurs opérations financières.**
Nous proposons trois types de solutions :

la Panoplie de ressources pour la surveillance des marchés du CGAP
Le CGAP a mis au point une panoplie de ressources à l'attention des organismes de régulation des marchés ainsi que d'autres acteurs, qui inclut des analyses de rapports statutaires, des examens de plaintes, des évaluations mystère et des enquêtes téléphoniques. Cet outil permet aux superviseurs d'évaluer les risques pour les consommateurs et, au besoin, de prendre les mesures correctives de rigueur.

Mécanismes pour porter la voix des consommateurs (CCV)
Le CGAP a mis en place trois mécanismes pour permettre aux consommateurs de partager leurs expériences et d'influer sur la réglementation : des groupes/associations de consommateurs ; des organes de réglementation consultatifs ; et des systèmes informatiques et médias sociaux. Il travaille actuellement sur des projets pilotes visant à montrer comment ces mécanismes peuvent autonomiser le consommateur.

Mise à l'honneur de prestataires de SFN responsables
Le CGAP met en avant les prestataires de SFN qui placent le client au cœur de leurs préoccupations et adoptent des modèles commerciaux responsables ainsi que des canaux de distribution (agents) qui protègent le consommateur et ses données.

Ressources liées au CGAP :

Document travail : Tenir compte de la voix des consommateurs (CCV) au moment d'élaborer la réglementation financière

Document travail : Placer davantage le client au centre de la réglementation sur la protection du consommateur

Leadership Essay: "It's Time to Change the Equation on Consumer Protection."

Série de blogs : Cybersecurity and Financial Inclusion: Protecting Customers, Building Trust.

Article de blog : Inde – Examen des médias sociaux pour déceler les risques que présente le crédit numérique pour le consommateur

Veuillez consulter l'annexe pour les solutions mises en œuvre par d'autres organisations

ANNEXES

LISTE DÉTAILLÉE : RISQUES DANS LES QUATRE GRANDES CATÉGORIES

FRAUDE	UTILISATION ABUSIVE DES DONNÉES	MANQUE DE TRANSPARENCE	INADÉQUATION DES MÉCANISMES DE RECOURS
• Fraude par échange de cartes SIM/prise de contrôle de comptes • Fraude interne (par ex. : accès non autorisé aux informations du client, perception non réglementaire de frais) • Fraude par identité synthétique • Fraude par carte (par ex. : paiement à distance, contrefaçon) • Fraude par identité biométrique • Fraude par application mobile/espionnage de smartphones • Investissements numériques non agréés/ pyramide de Ponzi • Fraude par ingénierie sociale (par ex. : hameçonnage – y compris messages SMS et messages vocaux –, usurpation d'identité) • Fraude par les réseaux sociaux (par ex. : Facebook, Twitter) • Fraude par transfert de fonds (par ex. : règlement anticipé non justifié, extorsion, arnaque aux sentiments, transfert prétendument incorrect) • Fraude par navigateur mobile/dévoiement • Dispositif contrefait • Compromission des infrastructures (par ex. : GAB/argent mobile) • Vol d'appareils mobiles/partage d'appareils • Arnaque au paiement par autorisation	• Biais algorithmique • Pratiques malhonnêtes (par ex. : vente de produits inadaptés, marketing agressif/ventes croisées, pratiques abusives de recouvrement de dettes, notamment par intimidation sociale) • Intrusion dans la vie privée • Prises de décisions opaques • Violation de données (avec accroissement des cyberrisques) • Consentement non éclairé • Profilage imprécis et absence d'intégrité des données • Effet Mathieu • Risque lié au partage des responsabilités • Incapacité du prestataire de services de paiement numérique de protéger les données personnelles du client • Incapacité du client de protéger ses données personnelles • Pratiques de gestion des données non dévoilées	• Information sur la tarification floue/incomplète • Pratiques malhonnêtes (par ex. : vente de produits inadaptés, marketing agressif/ventes croisées, pratiques abusives de recouvrement de dettes, notamment par intimidation sociale) • Menu/interface utilisateur complexe/déroutant(e) • Tarification/modalités et conditions inaccessibles, présentation compliquée des états financiers • Impossibilité de comparer des produits • Frais cachés/non expliqués/non dévoilés • Pratiques de gestion des données non dévoilées • Langue juridique complexe et volume excessif d'informations, qui dépasse/déroute le consommateur • Aucun protocole concernant les références • Risques inhérents aux produits non communiqués au client. • Publicité trompeuse	• Procédures de dépôt de plaintes floues • Dispositifs de gestion de plaintes onéreux • Procédures de dépôt de plaintes chronophages • Lenteur des procédures de recours • Personnel peu réactif ou mal formé • Absence de canaux appropriés pour la notification de problèmes • Difficulté à résoudre des différends transfrontaliers • Solutions incomplètes ou insuffisantes en cas de différends • Agents non formés et non encadrés • Normes sociales

LISTE DÉTAILLÉE : RISQUES TRANSVERSAUX DANS DEUX CATÉGORIES

RISQUES LIÉS AUX AGENTS	PANNE DE RÉSEAU
• Moins d'agents femmes • Normes sociales • Moins d'agents en milieu rural • Fraude/surfacturation/marge sur frais/frais non autorisés • Accès au code PIN du client (vol/compromission) • Solution insatisfaisante proposée par les agents en cas de différends • Connaissance limitée des produits • Manipulation des clients • Traitement injuste des clients/discrimination selon le statut social • Liquidité insuffisante des agents, susceptible d'entraîner un fractionnement, un refus de transactions ou des paiements en bloc • Agents non formés et non encadrés	• Attaques par déni de service distribué • Infrastructure des SFN inadéquate • Mise à niveau des systèmes insuffisamment éprouvée • Coupures de courant • Plans inadéquats pour assurer la reprise après sinistre et la poursuite des activités • Comportement risqué du client (par ex. : confier du liquide, son code PIN ou son téléphone à un tiers) • Transactions incomplètes ou interrompues/fonds inaccessibles • Absence de messages de confirmation – avec le risque de dupliquer la transaction • Plaintes en souffrance (par ex. : l'agent/prestataire de services ne vérifie pas l'état de la transaction ou ne prend pas contact avec le prestataire de SFN)

GLOSSAIRE

Risques liés aux agents – Risques issus des interactions entre l'utilisateur de SFN et l'agent désigné par le prestataire de SFN.

Cybersécurité – Pratique qui consiste à protéger d'attaques malveillantes les ordinateurs, les serveurs, les appareils mobiles, les réseaux et les données.

Usage abusif des données – Risque qu'une entité ou une personne utilisent les données ou les informations d'un client de SFN à des fins autres que celles prévues initialement.

Services financiers numériques (SFN) – Tous les services financiers fournis par les circuits numériques qui alimentent les dispositifs tels que les téléphones portables, les GAB, les terminaux point de vente, les appareils de communication en champ proche, les puces, les cartes électroniques, les dispositifs biométriques, les tablettes et les phablettes, ainsi que d'autres circuits – qu'il s'agisse d'épargne, de paiements, de crédits, d'assurances, de transferts, d'investissements ou de toute autre opération de ce type. Ils incluent les services accessibles par l'entremise d'agents ou de réseaux tiers.

Risques des SFN pour le consommateur – Toute situation ou tout élément qui entraîne pour un consommateur une perte ou un préjudice potentiel ou réel (financier ou non) lorsqu'il utilise des SFN.

Fraude – Risque qu'une entité ou une personne se livre sciemment à des actions malintentionnées qui occasionneront une perte financière pour le consommateur de SFN.

Manque de transparence – Risque pour un client de se voir proposer, en rapport avec des SFN, des termes, des modalités, des frais ou d'autres conditions qu'il ne comprend pas.

Inadéquation des mécanismes de recours – Risque pour un utilisateur de SFN de ne pas disposer des canaux nécessaires pour déposer une plainte, ou de constater que cette dernière n'est pas dûment traitée.

Panne de réseau – Risque qu'un problème technique empêche un client d'utiliser les SFN

Surendettement* – Un individu ou un ménage est surendetté lorsque ses ressources disponibles ou prévues sont insuffisantes pour tenir ses engagements sans devoir réduire son train de vie.

Clients vulnérables –** Clients ou groupes de clients à faible revenu davantage livrés à eux-mêmes comme, par exemple, les jeunes, les personnes âgées, les femmes, les populations rurales et les réfugiés. Le programme de protection des consommateurs du CGAP accorde une importance particulière aux femmes et aux populations rurales.

* Adapté de Household Overindebtedness Definition and measurement with Italian Data de Giovanni D'Alessio et Stefano Iezzi
** Le CGAP reconnaît que la vulnérabilité peut faire l'objet d'autres définitions. Par exemple, la Financial Conduct Authority définit un client vulnérable comme quelqu'un qui, en raison de circonstances personnelles, peut facilement être la cible d'actions préjudiciables, en particulier lorsqu'une société ne prend pas les précautions d'usage.

MÉTHODE DE RECHERCHE

Examinés
175 publications/articles

- 94 publications font état d'une augmentation ou d'une diminution des risques ; 81 mentionnent uniquement la nature des risques
- 40 publications et articles supplémentaires (avantages des SFN, solutions, etc.)
- Veuillez vous référer à la section Références pour une liste des publications et des articles.

Consultés
74 experts nationaux, régionaux et mondiaux dans 33 institutions

- Groupes de réflexion/institutions de recherche
- Bailleurs de fonds/investisseurs
- Associations professionnelles
- Prestataires
- Entités chargées des stratégies/de la supervision
- Veuillez vous référer aux diapositives 52, 53 et 54 pour une liste des institutions et des personnes consultées.

Insertion des informations communiquées par les experts

- Les premières conclusions ont rencontré l'assentiment de la plupart des experts
- Mise à jour de certaines sections
- Ajout de plusieurs nouvelles sections

CONSULTATIONS

Organisation	Personnes consultées	Désignation
Alliance pour l'inclusion financière (AIF)	Ghiyazuddin Mohammad	Directeur de stratégie, Services des finances numériques
	Luis Trevino Garza	Directeur de stratégie, Application de données et implantation à l'échelon national
	Sulita Levaux	Spécialiste des stratégies, Autonomisation des consommateurs et pratiques de marché
Banque des règlements internationaux (BRI)	Jon Frost	Économiste principal, Technologie financière et innovation numérique, Département d'économie numérique
Better than Cash Alliance	Camilo Tellez	Directeur, Innovation numérique
	Keyzom Ngodup	Directeur, région asiatique
Fondation Bill & Melinda Gates	Anna Wallace	Directrice, Protection des consommateurs et technologie réglementaire
	Deon Woods Bell	Conseillère principale, Stratégie
	Pawan Bakhshi PhD	Directeur Inde, Services financiers pour les pauvres
Caribou Digital	Marissa Dean	Directrice, Investissements numériques
CDC Group	Machal Karim	Directrice, Investissements d'impact dans le développement
Center for Effective Global Action	Marisa McKasson	Attachée principale de programmes
	Leah Bridle	Directeur associé de recherches
Center for Financial Inclusion	Alexandra Rizzi	Directrice principale de recherches, Données de consommation, créneaux et risques
Consumer Financial Protection Bureau (CFPB), États-Unis d'Amérique	Mary Griffin	Directrice exécutive - Cooperative Development Foundation, ex-Conseillère principale - Office of Community Affairs at CFPB
Consumers International	Antonino Serra Cambaceres	Directeur, Activités de plaidoyer
	Matthew Jones	Spécialiste de projet
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)	Klaus Prochaska	Directeur, Développement du secteur financier et des assurances, siège de GIZ
	Florian Berndt	Conseiller en chef, Développement de systèmes financiers, inclusion financière et finance responsable
	Saliya Kanathigoda	Conseiller programme, finance numérique
	Marian Engelbarts	Conseiller à l'élaboration de systèmes financiers
Dvara Research	Indradeep Ghosh	Directeur exécutif
	Deepti George	Directrice exécutive adjointe et directrice de stratégie
	Beni Chugh	Directrice, activités de recherches

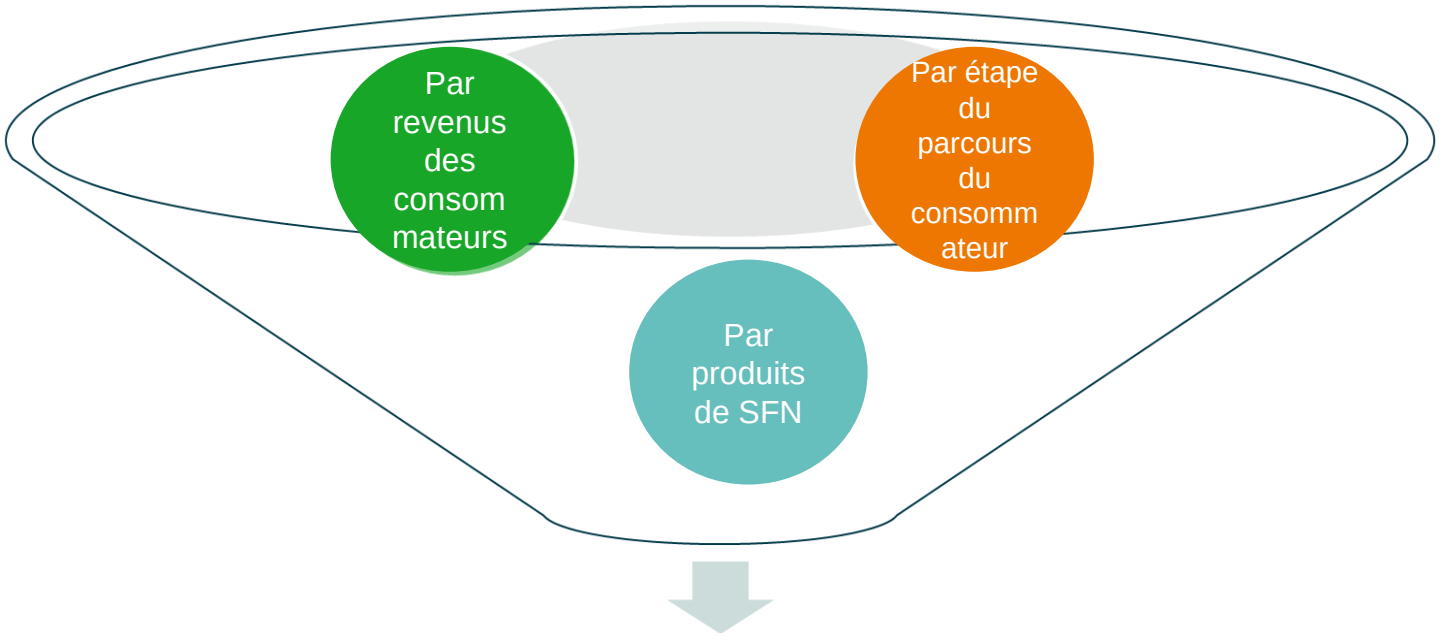
CONSULTATIONS (suite)

Organisation	Personnes consultées	Désignation
Enhancing Financial Innovation and Access (EFInA) Nigeria	Henry Chukwu	Spécialiste de programme, Services financiers numériques
Financial Sector Deepening (FSD) Zambie	Betty Wilkinson	Directeur général
	Charity Chikumbi	Directrice, Département de stratégies et de finances numériques
	William Sichombo	Chef, Département de stratégies et de finances numériques
Financial Sector Deepening (FSD) Afrique	Shakila Kerre	Spécialiste de l'économie numérique
Flourish Ventures	Stella Klemperer	Directrice de stratégie
	Tina Moran	Analyste principale des investissements
GSM Association (GSMA)	Saad Farooq	Gestionnaire principal, plaidoyer (paiement mobile)
	Ashley Olson Onyango	Directrice du département d'inclusion financière, Agritech
	Julianne Mweheire	Directrice des données, Programme de paiement mobile
	Brian Muthiora	Chef des activités statutaires et stratégiques, Programme de paiement mobile
	Claire Sibthorpe	Directrice des femmes connectées, de la société connectée et des technologies d'assistance
	Daniele Tricarico	Directeur de recherche et d'analyse des connaissances, Agritech
	Sonia Pietosi	Directeur du département des connaissances, Agritech
Innovation for Poverty Action (IPA)	Rafe Mazer	Directeur de projet, protection des consommateurs
	Daniel Putman	Postdoctorants, Projet de protection des consommateurs
	Rebecca Rouse	Directrice de programme, Programme d'inclusion financière
International Finance Corporation (IFC)	Lory Camba Opem	Chargée d'opérations et cheffe de la finance responsable
Union internationale des télécommunications (UIT)	Venkatesen Mauree	Coordinateur de programme, Département des groupes d'études, Bureau de normalisation
	Bilel Jamoussi	Directeur, Département des groupes d'études
Mastercard Center for Inclusive Growth	Daniel Barker	Vice-président pour la recherche et les connaissances
	Ali Schmidt-Fellner	Gestionnaire des connaissances
	Leslie Meek-Wohl	Directrice des programmes mondiaux
MicroSave Consulting (MSC)	Elizabeth Berthe	Conclusion de l'examen annuel de l'OEG.
	Graham Wright	Fondateur et Directeur de gestion des groupes (MSC)

CONSULTATIONS (suite)

Organisation	Personnes consultées	Désignation
Observatoire de la qualité des services financiers (Sénégal)	Habib Ndao	Secrétaire exécutif
	Dr Aliou Diop	Expert financier
Orange	Anne Catherine Tchokonté	Directrice de la diversification des services financiers mobiles, Moyen-Orient et Afrique
Peruvian Financial Regulatory Authority	Elias Roger Vargas Laredo	Intendant adjoint du suivi des marchés et des taux d'intérêt
	Mariela Zaldivar	Intendant adjoint du suivi des marchés et de l'inclusion financière
Social Performance Task Force (SPTF)	Anton Simanowitz	Directeur de la centricité des clients
	Laura Foose	Directeur exécutif
	Amelia Greenberg	Directrice adjointe du mécanisme pour une finance inclusive et responsable, Afrique et Moyen-Orient
	Katie Hoffman	Directrice du mécanisme pour une finance inclusive et responsable, Asie du Sud-Est
Fonds des Nations Unies pour l'enfance (UNICEF)**	Ahmed Dermish	Spécialiste principal, stratégies et plaidoyer, écosystèmes numériques inclusifs
	Alexis Ditkowsky	Spécialiste des livraisons rapides
	Naomi Bourne	Analyste de stratégies, finance numérique
	Jeremiah Grossman	Spécialiste de la stratégie numérique
Avocate spéciale du Secrétaire général des Nations Unies pour la finance inclusive pour le développement (UNSGSA)	Pia Tayag	Director
	Peter McConaghy	Conseiller stratégique, Secteur de la finance
	David Symington	Conseiller stratégique, Technologie financière et paiements numériques
	Nancy Widjaja	Conseillère stratégique, Santé financière et participation du secteur privé
Agence américaine pour le développement international (USAID)	Paul Nelson	Conseiller principal en finance numérique
Visa	Amina Tirana	Directrice de stratégies et de mesure, Impact social
Équipe de protection du consommateur de la Banque mondiale	Jennifer Chien	Spécialiste principal du secteur financier
	Gian Boeddu	Spécialiste principal du secteur financier
Banque mondiale G2PX.	Vyjayanti T. Desai	Gestionnaire de pratiques
	Georgina Marin	Chargé de programme
	Minita Mary Varghese	Consultante
Women's World Banking	Sonja Kelly	Recherches et plaidoyer en faveur de l'inclusion économique des femmes

AUTRES TYPOLOGIES DE RISQUES PRISES EN CONSIDÉRATION



Choisir les quatre grands types de risques liés au service d'une clientèle variée

AUTRES EXEMPLES : ÉVOLUTION DES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

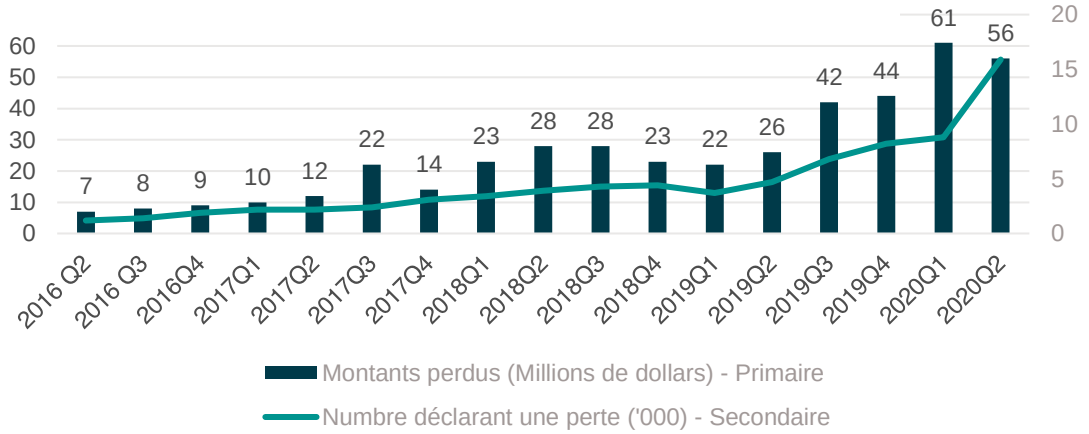
Le volume et les effets des arnaques dans les médias sociaux connaissent une augmentation rapide.

Une étude, menée par Consumers International (2019) dans neuf pays, a mis en lumière des arnaques à l'investissement et des arnaques par usurpation, ces deux types d'escroquerie étant les plus fréquents dans les médias sociaux.

Près de 4 milliards de personnes (soit environ 50 % de la population mondiale) utilisent des plates-formes comme Facebook, Twitter, WhatsApp et Instagram (Statista 2021). Les médias sociaux offrent une occasion rêvée aux escrocs pour leurrer les utilisateurs de SFN peu méfiants. Consumers International indique également que la Swedish Consumer Agency a découvert que certaines personnes qui souffraient d'un handicap physique ou cognitif, percevaient de faibles revenus ou avaient un niveau d'éducation ainsi que des compétences linguistiques limités, étaient plus susceptibles de souscrire des abonnements piège.

Consumers International note par ailleurs que, selon les données de l'Australian Competition and Consumer Commission, les sommes perdues au titre d'escroqueries dans les médias sociaux, ont été multipliées par quatre entre 2015 et 2018, passant de 3,8 millions à 13,1 millions de dollars australiens

Escroqueries dans les médias sociaux, 2016–2020



Source : Federal Trade Commission Consumer Protection Data Spotlight, octobre 2020.

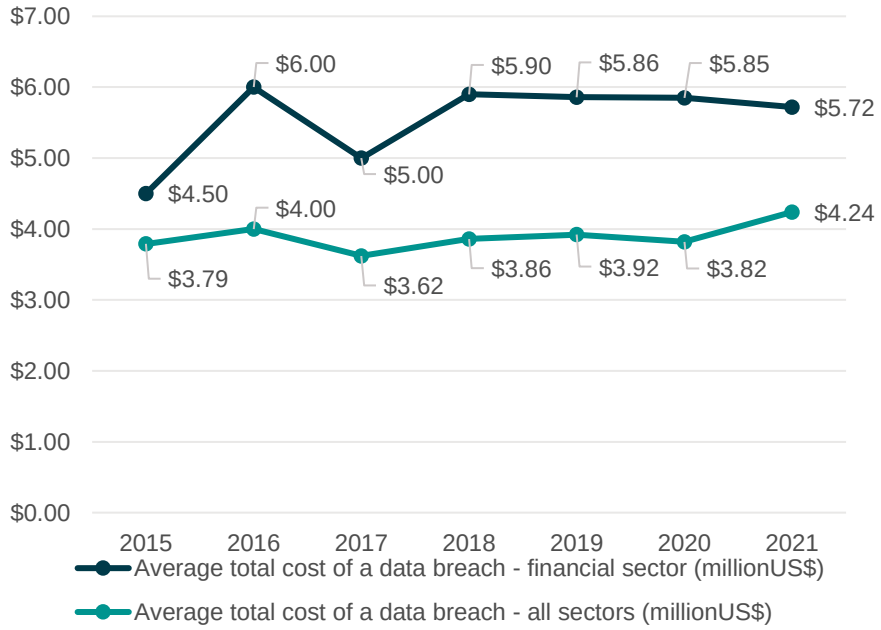
Aux États-Unis d'Amérique, les données de la Federal Trade Commission (2020) font état d'escroqueries sur les médias sociaux et indiquent que les sommes perdues à ce titre ont augmenté en flèche entre 2016 et 2020.

Dans les pays émergents ainsi que ceux en développement, plusieurs médias ont évoqué le cas de personnes victimes d'escroqueries dans les médias sociaux. Toutefois, les données permettant d'évaluer l'évolution de ce phénomène ne sont pas encore disponibles.

AUTRES EXEMPLES : ÉVOLUTION DES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

Les occasions commerciales manquées représentent la majeure partie des coûts inhérents aux violations de données, indiquant que ces dernières peuvent entraîner une perte de confiance dans le secteur financier formel.

Coût total moyen des violations de données, 2015-2021



Source : Adapté des IBM's Cost of a Data Breach reports, 2016 à 2021.

Bien que le coût total moyen des violations de données n'ait pas substantiellement augmenté depuis 2015, le secteur financier a systématiquement enregistré un coût total moyen supérieur à celui de tous les autres secteurs. Cependant, il convient de noter qu'en 2020 et 2021, le coût moyen d'une violation de données, tous secteurs confondus, s'est accru de 11 % tandis que le coût moyen dans le secteur financier a baissé de 2,2 %. Cette légère amélioration dans la finance peut s'expliquer par le renforcement des mesures de cybersécurité que les différents acteurs ont adoptées.

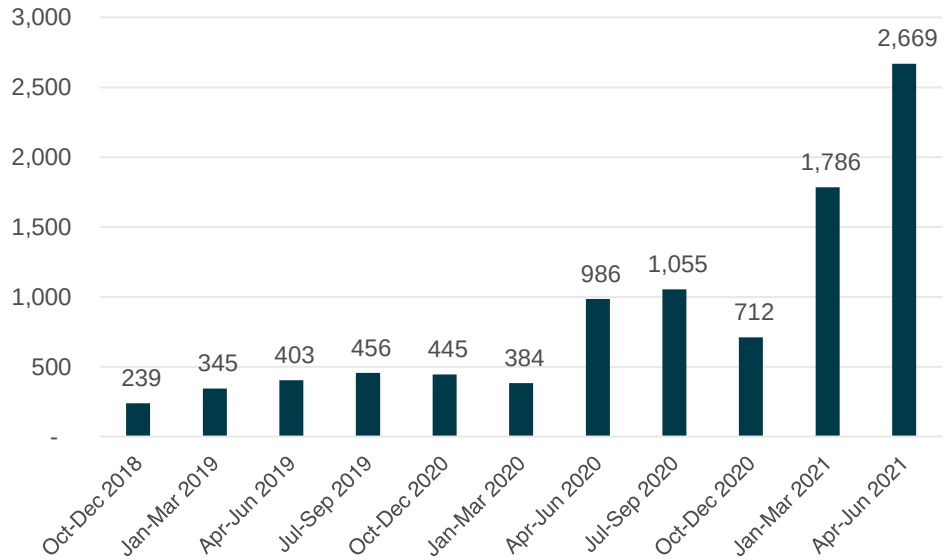
Pour calculer le coût total d'une violation de données, IBM tient compte des dépenses telles que les abonnements à un service de suivi de la solvabilité, les promotions sur des produits/ventes à venir ainsi que la clientèle perdue et les occasions commerciales manquées.

En 2020–2021, à 38 %, les occasions commerciales manquées représentaient la plus grande partie des coûts occasionnés par la violation de données. Ces chiffres montrent aux acteurs de l'inclusion financière que la publication des données des clients pourraient entraîner une perte de confiance dans le secteur financier et contribuer, à terme, à l'exclusion financière.

AUTRES EXEMPLES : ÉVOLUTION DES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

Les plaintes concernant les porte-monnaie électroniques et les paiements mobiles sont en augmentation, mais les mesures de protection du consommateur ne suivent pas la même tendance.

Plaintes relatives aux paiements mobiles et aux porte-monnaie électroniques aux États-Unis d'Amérique, 2017-2021



Source : Compilé par les auteurs qui ont utilisé les données de la base du CFPB sur les plaintes des consommateurs

Un examen des plaintes relatives aux porte-monnaie électroniques/paiements mobiles, reçues par le Consumer Financial Protection Bureau (CFPB 2021)* ,montre qu'elles ont connu une augmentation substantielle à partir du mois de mars 2020, ce qui coïncide avec la première vague de la pandémie de COVID-19. Sur les 9480 plaintes reçues entre octobre 2018 et juin 2021, 76 % (7208) ont été déposées après le mois de mars 2020. La majeure partie concernait la gestion/ouverture/ fermeture d'un porte-monnaie électronique (45 %), suivie des fraudes/escroqueries (23 %) et des transactions non autorisées (22 %).

Mierzwinski et al.Mierzwinski et al. (2021) constatent que, bien que les sites Web des applications de paiement mettent en garde les consommateurs contre les escroqueries, ils offrent peu de possibilités de recours aux victimes de fraude. En outre, contrairement aux cartes de crédit – régies par le Truth In Lending Act et le Fair Credit Billing Act – et aux cartes de débit – qui sont couvertes par l'Electronic Fund Transfer Act (EFTA) – aucune réglementation ne s'applique aux transactions P2P. Bien que l'EFTA englobe ces dernières, il ne s'applique pas toujours nécessairement.

Si un pays développé comme les États-Unis d'Amérique doit faire face à des problèmes de recours, nous en déduisons que le scénario doit être pire dans les pays émergents et en développement.

*Organe indépendant aux États-Unis d'Amérique, le CFPB est chargé de la protection des consommateurs dans le secteur financier. Il prend en charge les plaintes auxquelles les prestataires de SFN ne peuvent apporter aucune réponse.

EXEMPLES : SOLUTIONS POUR ATTÉNUER LES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

La plupart des solutions qui s'imposent peu à peu sont fondées sur la technologie.

Veuillez noter que les exemples présentés dans cette section sont empiriques , l'étude n'étant pas centrée sur la quête de solutions.

Les systèmes de détection fondés sur l'intelligence artificielle (IA) peuvent aider à repérer et à atténuer les fraudes (Experian 2020 ; FSB 2017 ; Calzolari 2021). En outre, les organismes de supervision peuvent utiliser l'IA pour déceler les fraudes dans le secteur financier.

Par exemple :

- L'Australian Securities and Investments Commission (ASIC) a recours au traitement du langage naturel classique et à d'autres techniques pour repérer et extraire les fragments d'intérêt.
- La Monetary Authority of Singapore (MAS) explore les possibilités d'utiliser l'IA et l'apprentissage automatique pour détecter et examiner les transactions douteuses qui méritent un suivi.
- La United States Securities and Exchange Commission (SEC) utilise l'analytique des données massives et les algorithmes d'apprentissage automatique pour repérer tout comportement suspect ou toute fraude éventuels.

Les actions de sensibilisation menées par les organismes de supervision du secteur financier ainsi que les organismes chargés de l'application des lois ont contribué, dans certains cas, à atténuer les fraudes. Par exemple, certains rapports* de presse publiés en 2020 indiquent que les Émirats Arabes Unis ont observé une diminution des fraudes liées à l'échange de cartes Sim après que la banque centrale et la police ont lancé une vaste campagne de sensibilisation à l'échelon national.

Compte tenu des recherches menées par Buku et Mazer (2017), le CGAP recommande l'adoption des mesures suivantes afin d'atténuer les fraudes dans les services financiers mobiles :

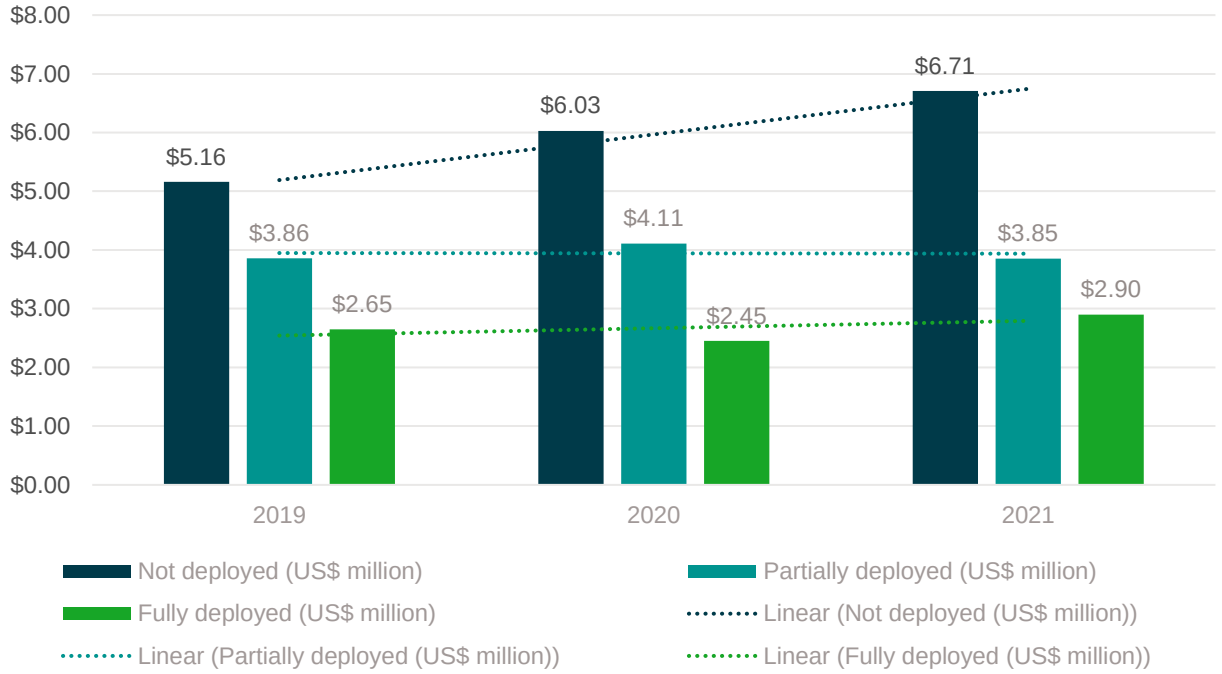
- Programmes exhaustifs de gestion des fraudes
- Programme de gestion, de formation et de recrutement d'agents, ainsi que de suivi de la conformité
- Incorporation de l'évaluation des risques d'un produit dans les programmes de gestion des risques
- Mesures exhaustives de prévention de la fraude commise par les agents (par ex. : formation et sensibilisation)
- Mise en place d'un dispositif efficace pour d'examen des plaintes
- Recrutement efficace de personnel

*Rapports émanant de Emirates News Agency, WAM, Emirati News et Gulf News.

EXEMPLES DE SOLUTIONS POUR ATTÉNUER LES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

Les investissements dans l'IA et l'automatisation aux fins de sécurité, peuvent réduire considérablement le temps moyen nécessaire pour repérer une violation de données et y apporter une réponse.

Coût moyen d'une violation de données par niveau de déploiement de l'IA aux fins de sécurité



Le rapport Cost of a Data Breach Report publié par IBM en 2021 montre que les sociétés qui ont recours à l'IA (par ex. système de détection de fraude) et à l'automatisation, gagnent des journées entières lorsqu'elles sont amenées à détecter et à neutraliser une violation de données. Par exemple, en 2021, les sociétés utilisant l'IA et l'automatisation ont mis en moyenne 247 jours pour repérer et déjouer une opération de violation de données, alors que les firmes ne disposant pas de ces techniques ont mis 324 jours.

En outre, les sociétés ayant recours à l'IA et à l'automatisation ont supporté en moyenne, en 2021, des coûts 80 % inférieurs (US$2,91 millions) pour lutter contre ce fléau, par rapport à celles qui n'ont pas misé sur ces outils.

En trois ans, ces dernières ont également connu une augmentation plus importante des coûts liés à la violation de données.

Source : Adapté des IBM's Cost of a Data Breach Reports, 2021.

EXEMPLES DE SOLUTIONS POUR ATTÉNUER LES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

Autres solutions pour atténuer l'usage abusif des données

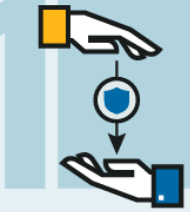
Approches pour atténuer les biais algorithmiques

Adopter des stratégies nationales visant à intégrer l'utilisation de l'IA, qui tiennent compte de considérations éthiques. En 2017, le Canada a été le premier pays à publier une stratégie nationale sur l'intégration de l'IA. Dès le mois de décembre 2020, plus de 30 pays avaient suivi l'exemple du Canada, notamment la Chine, le Japon, la France, l'Allemagne, l'Inde, le Mexique, l'Estonie, les États-Unis d'Amérique, la Russie et l'Indonésie. D'autres, comme le Brésil, l'Argentine, le Kenya et la Malaisie, ont annoncé leur intention d'élaborer des stratégies similaires (Daniel et al. 2021).

Réalisation d'audits algorithmiques En 2020, une cour fédérale des États-Unis d'Amérique a statué que « des recherches indépendantes, visant à déterminer si des algorithmes en ligne entraînaient des discriminations de race, de genre ou autres, ne violaient pas le Computer Fraud and Abuse Act » (Rizzi et al. 2021 ; Deloitte 2020 ; Kassir 2020 ; Calzolari 2021 ; Andrews 2021, FSB 2017). Toutefois, les audits algorithmiques exigent une expérience et des compétences que la plupart des auditeurs et des superviseurs financiers ne possèdent pas à l'heure actuelle.

Se fondant sur une recherche menée par Medine et Murthy (2020), le CGAP recommande :

1



Placer la responsabilité sur le fournisseur
Placer de nouvelles responsabilités sur les collecteurs et les traiteurs de données, plutôt que de se fier au consentement des consommateurs Deux possibilités :

Critère du but légitime
Utilisation des données autorisée uniquement quand elle profite au consommateur

OU

2

Charte des droits numériques
Donner aux consommateurs les moyens de contrôler leurs propres données en leur permettant d'accéder aux données, de les corriger et de les déplacer gratuitement.

Obligation fiduciaire
Toujours agir dans l'intérêt du consommateur

3

Représentants chargés de la protection des renseignements personnels
Veiller à l'équité dans le traitement des données par le biais de représentants chargés de protéger les renseignements personnels qui peuvent examiner les profils des données des consommateurs et vérifier les modèles algorithmiques en matière d'équité, de biais et d'exclusion

EXEMPLES DE SOLUTIONS POUR ATTÉNUER LES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

Les consommateurs, les prestataires de FSN et les organismes de supervision peuvent recourir aux médias sociaux pour gérer les plaintes et cerner les principales questions relatives à la protection du consommateur.

Exemples d'outils d'« écoute sociale » : tableau de bord analytique sur les plates-formes de médias sociaux et outils commerciaux

Innovation for Poverty Action (IPA) et Citibeats (2021) ont recueilli au Nigéria, au Kenya et en Ouganda des données sur les médias sociaux de Twitter, de Facebook et de Google Play Store pour comprendre les problèmes auxquels font face les consommateurs de SFN.

Sur les 4,5 millions de messages de médias sociaux récupérés de banques commerciales, de sociétés de télécommunications, de jeunes pousses de la technologie et des finances, ainsi que d'institutions spécialisées dans la microfinance, entre le 1er juillet 2019 et le 1er juillet 2020, l'analyse de texte et l'intervention humaine ont permis de déterminer les principaux problèmes auxquels sont confrontés les consommateurs. Il a notamment été constaté que :

- Les consommateurs de SFN utilisent principalement Twitter et Facebook pour la notification de toute question liée à leur protection, en particulier à l'assistance aux clients. Google Play est utilisé pour la notification de problèmes techniques.
- Les prestataires de services répondent lorsque les clients les informent de problèmes via les médias sociaux, mais le taux de réponse varie considérablement. Ce taux est plus important sur Facebook (5 à 46 %) et Google Play (8 à 58 %) que sur Twitter (0,04 à 1,2 %).

Aux Philippines, un agent conversationnel, appelé BSP's Online Budd, permet aux clients de déposer une plainte par les médias sociaux et d'autres plates-formes de communication. Il a recours à l'IA comme l'apprentissage automatique et le traitement du langage naturel, pour traiter ces plaintes et répondre directement ou faire remonter la demande jusqu'à un centre d'appel qui l'intègre dans une base de données (Duflos, Griffin et Valenzuela 2021).

Selon un sondage de l'American Bankers Association, 63 % des banques utilisent déjà les médias sociaux pour superviser les plaintes et ce, à des fins de gestion du risque, tandis que 12 % d'entre elles envisagent de procéder de la sorte dans les un à deux ans à venir (Banque mondiale 2019).

Toutefois, le recours aux médias sociaux peut présenter d'autres risques pour les prestataires et les consommateurs de SFN (se reporter aux lignes directrices de 2013 sur les médias sociaux du Federal Financial Institutions' Examination Council). En outre, les médias sociaux ne sont guère efficaces pour les consommateurs moins portés sur l'informatique, comme les femmes à faible revenu et les populations rurales qui, de manière générale, ne les utilisent pas.

Le CGAP a récemment mené une étude, en utilisant les données de Twitter et de Google Play Store afin de déterminer les principaux problèmes auxquels font face les consommateurs de crédits numériques en Inde.

Cette étude a eu recours au traitement du langage naturel et a appliqué la typologie des risques pour le consommateur, tel qu'elle est décrite dans le présent document, afin de classer les problèmes dans différentes catégories (Duflos et al. 2021a, 2021b).

EXEMPLES DE SOLUTIONS POUR ATTÉNUER LES RISQUES QUE PRÉSENTENT LES SFN POUR LE CONSOMMATEUR

Les programmes d'éducation financière peuvent atténuer certains risques, mais tout dépend du mode de prestation

Selon l'OCDE (2017), rares sont les programmes d'éducation financière axés sur les SFN qui répondent aux besoins des groupes vulnérables.

Arménie (milieu rural)

Contributions des ateliers de deux jours sur l'éducation financière

- À court terme, les ateliers ont eu un effet positif majeur sur la littératie financière et la confiance (AFI 2018).
- Six mois plus tard, cet effet était moins tangible, laissant supposer qu'il deviendrait négligeable à long terme (AFI 2020).

Malawi (milieu urbain)

Contributions du module de réponse vocale interactive, axé sur la littératie financière et destiné à informer les clients de l'importance de comprendre les conditions régissant l'octroi d'un crédit, le remboursement ainsi que les frais connexes

- Le module de réponse vocale interactive a permis aux consommateurs de mieux comprendre les notions de commissions sur le crédit, de remboursement de prêts à court terme, et de multiplication d'emprunts.
- Une amélioration du bien-être des d'emprunteurs a également été constatée (Robinson et Dupas 2020).

Tanzanie (milieu rural)

Contributions du support d'apprentissage interactif et personnalisé par message SMS, fondé sur les réponses et les préférences des consommateurs

- Les agriculteurs qui se sont rendus sur la plate-forme d'apprentissage ont réalisé cinq fois plus d'économies que ceux qui n'y ont pas accédé.
- Les agriculteurs qui se sont rendus sur la plate-forme d'apprentissage ont contracté des emprunts plus importants et remboursé leurs crédits à un rythme plus soutenu, que ceux qui n'y ont pas accédé.
- Les agriculteurs, qui ont exploré davantage de pages, ont affiché une plus grande activité financière (Mazer 2016).

RÉFÉRENCES

RÉFÉRENCES

Accenture. 2018. “Unmask Digital Fraud. Today. Boosting Customers' and Companies' Defense Against Digital Fraud.” White paper.

AFI. 2017. “Digitally Delivered Credit: Consumer Protection Issues and Policy Responses to New Models of Digital Lending.” AFI Consumer Empowerment and Market Conduct (CEMC) Working Group, Responsible Lending Sub-Group. Policy Guidance Note and Results from Regulators Survey.

AFI. 2018. “The Effectiveness of Short-term Financial Education Workshops in Rural Areas: The Case of Armenia.” Case study.

AFI. 2020. “The Long-term Effectiveness of Financial Education Classroom Workshops in Rural Areas: The Case of Armenia.” Case study.

Ahlström, Richard, and Fredrik Tjulander. 2020. “Insolvency Syndrome: When Over-indebtedness Affects Health and Wellbeing.” Finance Watch blog post.

Ahmed, Wajiha, and Natalia Gomes. 2015. “Papayas and Digital Finance: Emerging Consumer Risks in Colombia.” CGAP blog post.

Aite Group. 2021. “Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise.” Rapport.

American Bankers Association. 2019. “ Social Media in Banking 2019 Report.” Rapport.

Andrews, Dorothy. 2021. “Algorithmic Accountability.” National Association of Insurance Commissioners.

Annan, Francis. 2021. “Gender and Financial Misconduct: A Field Experiment on Mobile Money.” Georgia State University research paper.

Assolini, Fabio, and Andre Tenreiro. 2019. “Large-scale SIM Swap Fraud.” Securelist research.

Baur-Yazbeck, Silvia, and Jean-Louis Perrier. 2020. “Regional Centers Can Help Low-Income Countries Build Cyber Resilience.” CGAP blog post.

Baur-Yazbeck, Silvia, David Medine, and Jean-Louis Perrier. 2020. “Cybersecurity Resource Centers for the Financial Sector: A Proposed Business Concept.” CGAP FinDev Gateway slide deck.

BBC. 2020a. “Chinese Phones with Built-in Malware Sold in Africa.” Article.

BBC. 2020b. “U.S.-Government-issued Phones Run 'Chinese Malware'.” Article.

Better than Cash Alliance. 2021. UN Principles for Responsible Digital Payments: Building Trust, Mitigating Risks and Driving Inclusive Economies

Bharadwaj, Prashant, William Jack, and Tavneet Suri. 2019. “Fintech and Household Resilience to Shocks: Evidence from Digital Loans in Kenya.” NBER Working Paper 25604.

Biallas, Margarete, Momina Aijazuddin, and Lory Camba Opem. 2019. “The Case for Responsible Investing in Digital Financial Services.” IFC EMCompass Note 67.

BIS. 2019. “Welfare Implications of Digital Financial innovation.” Remarks by Luiz Awazu Pereira da Silvaat, Santander International Banking Conference, Madrid. Speech.

Bleszynska Katya. 2021. “Ponzi and Pyramid Schemes Spread Across Caribbean.” InSight Crime article.

Bold, Chris, and Rashmi Pillai. 2016. “The Impact of Shutting Down Mobile Money in Uganda.” CGAP blog post.

RÉFÉRENCES

Boshmaf, Yazan, Charitha Elvitigala, Husam Al Jawaheri, Primal Wijesekera, and Mashael Al Sabah. 2019. “Investigating MMM Ponzi Scheme on Bitcoin.” Technical Report.

Boyd, Mark. 2020. “Digital Finance APIs Come with Risks – Here's One Way to Manage Them.” CGAP blog post.

Bradsher, Keith, and Ailin Tang. 2017. “China to Debtors: Pay Up or Be Shamed.” New York Times article.

Breza, Emily, Martin Kanz, and Leora Klapper. 2017. “The Real Effects of Electronic Wage Payments: First Results.” International Growth Centre paper F-31407-BGD-1.

Buguroo. 2019. “Online Banking Fraud in Latin America: An Emerging Regional Threat.” White paper.

Buku, Mercy, and Rafe Mazer. 2017. “Fraud in Mobile Financial Services.” CGAP Brief.

Calzolari, Giacomo. 2021. “Artificial Intelligence Market and Capital Flows.” Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg. Study.

Carnegie Endowment for International Peace. 2020. “Timeline of Cyber Incidents Involving Financial Institutions.”

Carr, Brad, Pablo Urbiola, and Adrein Delle-Case. 2018. “Liability and Consumer Protection in Open Banking.” Institute of International Finance report.

CCAF, World Bank Group, and WEF. 2020. “The Global COVID-19 FinTech Market Rapid Assessment Study.” Rapport.

CEGA. 2016. “Access to Digital Credit and Its Spillover Effects in China.” Digital Credit Observatory (DCO) Results Brief.

CEGA. 2020. “Can Digital Credit Work for Agriculture? Lessons from Kenya and Uganda.” CEGA interview.

Central Bank of Kenya, Kenya National Bureau of Statistics, and FSD Kenya. 2019. “FinAccess Household Survey: Access, Usage, Quality and Impact.” Rapport.

CGAP and MSC. 2020. “Cash-in Cash-Out Cross-Country Analysis India.” Slide deck.

CGAP. 2018. “Financial Inclusion Insights Analytics: Côte D'Ivoire.” FinDev Gateway slide deck.

CGAP. Cybersecurity and Financial Inclusion: Protecting Customers, Building Trust. CGAP blog series.

Chalwe-Mulenga, Majorie, and Eric Duflos. 2021. “The Evolving Nature and Scale of Consumer Risks in Digital Finance.” CGAP blog post.

Chamboko, Richard, Robert Cull, Xavier Gine, Soren Heitmann, Fabian Reitzug, and Morne Van Der Westhuizen. 2020. “The Role of Gender in Agent Banking: Evidence from the Democratic Republic of Congo.” IFC and World Bank Policy Research Working Paper 9449.

Chen, Greg, and Rafe Mazer. 2016. “Instant, Automated, Remote: The Key Attributes of Digital Credit.” CGAP blog post.

Cheng, We Geng, Rodrigo de Oliveira Leite, and Fabio Caldieraro. 2021. “Financial Contagion in Internet Lending Platforms: Who Pays the Price?” Finance Research Letters.

RÉFÉRENCES

Chinese Academy of Financial Inclusion (CAFI). 2018. “Growing with Pain: Digital Financial Inclusion in China.” FinDev Gateway. Rapport.

Chivukula, Chinmayanand. 2021. “Consumer Grievance Redress in Financial Disputes in India.” Dvara Research.

Chugh, Beni. 2019. “Financial Regulation of Consumer-facing Fintech in India: Status Quo and Emerging Concerns.” Dvara Research Working Paper Series No. WP-2019-01.

Cisco. 2020. “Cisco Annual Internet Report (2018–2023).” White paper.

CNN Philippines. “SEC Shuts Down 11 More Online Lenders.” Article.

Coetzee, Gerhard. 2019. “It's Time to Change the Equation on Consumer Protection.” CGAP Leadership Essay.

Consumer Financial Protection Bureau (CFPB). 2021. “Consumer Complaint Database: Complaints by Sub-products, by Date Received by the CFPB.” Base de données.

Consumers International. 2017. “Banking on the Future: An Exploration of FinTech and the Consumer Interest.” Rapport.

Consumers International. 2019. “Social Media Scams: Understanding the Consumer Experience to Create a Safer Digital World.” Rapport.

Consumers International. 2021. “The Role of Consumer Organisations to Support Consumers of Financial sServices in Low and Middle Income Countries.” Consumers International and CGAP report.

Dabo, Mohamed. “Mobile Banking Statistics: The Future of Money Is in the Palm of Your Hand.” DataProt Retail Banker International Report.

Deloitte. 2020. “Algorithm Assurance: Ensuring that Algorithms Are Working as Needed.” Deloitte Malta report.

Duflos Eric, Daryl Collins, Jayshree Venkatesan, and Juan Carlos Izaguirre. 2021b. “Analyzing Social Media to Spot Digital Consumer Credit Risks in India.” CGAP blog post.

Duflos, Eric, Jayshree Venkatesan, Amulya Neelam, and Sarah Stanley. 2021a. “Digital Consumer Credit in India – Time to Take a Closer Look.” CGAP blog post.

Duflos, Eric, Mary Griffin, and Myra Valenzuela. 2021. “Elevating the Collective Consumer Voice in Financial Regulation.” CGAP Working Paper.

Dvara Research. 2020. “Future of Finance Initiative Conference Series 2019: Regulating Data-driven Finance).” Conference proceedings.

ESMA, EBA, and EIOPA. 2016. “Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions.” Joint Committee of the European Supervisory Authorities Discussion Paper.

Commission européenne. 2016. “Assessment of Current and Future Impact of Big Data on Financial Services.” Financial Service User Group paper.

Europol. 2020a. “Internet Organised Crime Threat Assessment (IOCTA) 2020.” European Union Agency for Law Enforcement Cooperation document.

Europol. 2020b. “The SIM Hijackers: How Criminals Are Stealing Millions by Hijacking Phone Numbers.” European Union Agency for Law Enforcement Cooperation article.

Experian. 2020. “2020 Global Identity and Fraud Report.”

Experian. 2021. “2021 Global Identity and Fraud Report.”

RÉFÉRENCES

Fahsbender Frederick. 2019. “A WhatsApp Audio Links Actress Jasmine Stuart with the Loom of Abundance.” Infobae article.

Farooq, Saad. 2019. “Mitigating Common Fraud Risks: Best Practices for the Mobile Money Industry.” GSMA paper.

Faux, Zeke. 2020. “Tech Startups Are Flooding Kenya with Apps Offering High-Interest Loans.” Bloomberg Businessweek article.

Federal Financial Institutions Examination Council. 2013. “Social Media: Consumer Compliance Risk Management Guidance.” Press release.

Federal Reserve Banks. 2021. “Synthetic Identity Fraud Defined.” Blog post.

Federal Trade Commission. 2020. “Scams Starting on Social Media Proliferate in Early 2020.” Consumer Protection Data Spotlight.

Ferreira, Mário, Filipa de Almeida, Jerônimo Soro, Márcia Maurer Herter, Diego Costa Pinto, and Carla Sofia Silva. 2021. “On the Relation Between Over-Indebtedness and Well-Being: An Analysis of the Mechanisms Influencing Health, Sleep, Life Satisfaction, and Emotional Well-Being.” Frontiers in Psychology paper.

FICO. 2018. “FICO Survey: 6 in 10 APAC Banks Say Use of Fraudulent 'Synthetic Identities' on the Rise.” Survey.

National Financial Inclusion Strategy (SNKI). 2018. Financial Inclusion Insights (FII) Indonesia. Rapport

Francis, Eilin, Joshua Blumenstock, and Jonathan Robinson. 2017. “Digital Credit: A Snapshot of the Current Landscape and Open Research Questions.” Centre for Effective Global Action and Bill & Melinda Gates Foundation research report.

Frost, Jon, Leonardo Gambacorta, and Romina Gambacorta. 2020. “The Matthew Effect and Modern Finance: On the Nexus Between Wealth Inequality, Financial Development, and Financial Technology.” BIS Working Paper No 871.

FSB. 2017. “Artificial Intelligence and Machine Learning in Financial Services.” Rapport.

FSD Kenya. 2019. “Digital Credit in Kenya: Facts and Figures from FinAccess 2019.” Focus Note.

Fu, Jonathan, and Mrinal Mishra 2020b. “Fintech in the Time of COVID-19: Trust and Technological Adoption During Crises.” Swiss Finance Institute Research Paper No. 20–38.

Fu, Jonathan, and Mrinal Mishra. 2020a. “Combating the Rise in Fraudulent Fintech Apps.” Center for Financial Inclusion blog post.

Garz, Seth, Xavier Giné, Dean Karlan, Rafe Mazer , Benjamin N. Roth, Rebecca Rouse, Caitlin Sanford, and Jonathan Zinman. 2021. “Consumer Financial Protection in Lower-Income Countries: A Review of the Evidence and Directions for Future Research.” NBER Working Paper 28262.

Genga, Kevin, Wanjiku Kiarie, and Vera Bersudskaya. 2018. “Measuring Risk in Agent Networks: What Risks Are Inherent in Agency Business and How to Track Them.” MicroSave Helix Institute of Digital Finance paper.

Gibbings Wesley. 2020. “The Caribbean's Pandemic Pyramids and Ponzis.” The Caribbean Investigative Journalism Network article.

Google Next Billion Users. 2021. “New Internet Users: Similar and Very Different.” Research.

RÉFÉRENCES

GPFI. 2020. “Advancing Women's Digital Financial Inclusion.” BTCA, Women's World Banking, and World Bank Group report.

GSMA. 2020. “MTN MoMo Pay Merchant Payments: Expanding Female Mobile Money Usage in Ghana.” Connected Women Case Study.

Harihareswara, Nandini, Zerubabel Junior Kwebiiha, Brian Katimbo, Anne Duijnhouwer, and Moïra Favrichon. 2019. “State of the Digital Financial Services Market in Zambia, 2018.” UNCDF and BoZ report.

Hayes, Marianne. 2020. “The Many Different Forms of Identity Theft.” Experian blog post.

Henderson, Roxanne, and Loni Prinsloo. 2021. “South African Brothers Vanish, and So Does $3.6 Billion in Bitcoin.” Bloomberg Wealth article.

Holly, Isaac, Kilyelyani Kanjo, Brian Katimbo, Anne Duijnhouwer, Moïra Favrichon, and Mali Kambandu. 2020. “State of the Digital Financial Services Market in Zambia, 2019: Results from the UNCDF Annual Provider Survey.” UNCDF and BoZ report.

Huang Li, Li Oliver Zhen, Lin Yupeng, Xu Chao and Xu Haoran. 2021.” Gender and Age-based Investor Affinities in a Ponzi Scheme.” Article.

Hurly, Mikella, and Julius Adebayo. 2017. “Credit Scoring in the Era of Big Data.” Yale Journal of Law and Technology article.

IBM. 2020. “Cost of a Data Breach Report 2020.” IBM Security and Ponemon Institute report.

IBM. 2021. “Cost of a Data Breach Report 2021.” IBM Security and Ponemon Institute report.

IDEO.org and the Bill & Melinda Gates Foundation. 2019. “Women and Money: Insights and a Path to Close the Gender Gap.” Rapport.

IDEO.org. 2020. “Measuring and Designing for Women's Financial Empowerment. Increasing Women's Voice, Influence, and Control of Money.”

SFI. 2018. “Closing the Gender Gap: Opportunities for the Women's Mobile Financial Services Market in Bangladesh.” Rapport.

IMF. 2020. “Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies.” IMF Special Series on COVID-19.

Institute and Faculty of Actuaries (UK) 2017. “Data Science in Insurance: Opportunities and Risks for Consumers.” Policy Briefing.

Interpol. 2021. “ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook from the ASEAN Cybercrime Operations Desk.”

IPA and Citibeats. 2021. “Social Media Usage by Digital Finance Consumers: Analysis of Consumer Complaints in Kenya, Nigeria, and Uganda. July 2019–July 2020.” IPA study.

IPA and Competition Authority of Kenya. 2021. “Kenya Consumer Protection in Digital Finance Survey.”

IPA and Uganda Communications Commission. 2021. “Uganda Consumer Protection in Digital Finance Survey.”

IPA. 2021. “Nigeria Consumer Protection in Digital Finance Survey.”

ITU. 2016. “Commonly Identified Consumer Protection Themes for Digital Financial Services.” ITU-T Focus Group Digital Financial Services.

RÉFÉRENCES

ITU. 2020. “Unlicensed Digital Investment Schemes (UDIS).” Financial Inclusion Global Initiative (FIGI) Security, Infrastructure, and Trust Working Group report.

Izaguirre, Juan Carlos, Denise Dias, Eric Duflos, Laura Newbury Brix, Olga Tomilova, and Myra Valenzuela. 2022. “Market Monitoring for Financial Consumer Protection.” CGAP toolkit.

Izaguirre, Juan Carlos, Michelle Kaffenberger, and Rafe Mazer. 2018. “It's Time to Slow Digital Credit's Growth in East Africa.” CGAP blog post.

Izaguirre, Juan Carlos, Rafe Mazer, and Louis Graham. 2018. “Digital Credit Market Monitoring in Tanzania.” CGAP slide deck.

Izaguirre, Juan Carlos. 2020. ”Making Consumer Protection Regulation More Customer-Centric.” CGAP Working Paper.

Jenik, Ivo, Timothy Lyman, and Alessandro Nava. 2016. “Will Crowdfunding Help Financial Inclusion of Unserved Crowds?” CGAP blog post.

Kabir, Raiyan, and Jeni Klugman. “Women's Financial Inclusion in a Digital World: How Mobile Phones Can Reduce Gender Gaps.” Georgetown Institute for Women, Peace and Security report.

Kafeero, Stephen. 2020. “Uganda's Banks Have Been Plunged Into Chaos by a Mobile Money Fraud Hack.” Quartz Africa article.

Kaffenberger, Michelle, Edoardo Totolo, and Matthew Soursourian. 2018. “A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania.” CGAP Working Paper.

Kaffenberger, Michelle. 2018. “Digital Credit in Tanzania: Customer Experiences and Emerging Risks.” CGAP.

Kassir, Sara. 2020. “Algorithmic Auditing: The Key to Making Machine Learning in the Public Interest.” IBM Center for the Business of Government Viewpoints article.

Kelly, Sonja, and Mehrdad Mirpourian. 2021. “Algorithmic Bias, Financial Inclusion, and Gender.” Women's World Banking.

Kiarie, Nancy, Ian Odongo, and Vera Bersudskaya. 2018. “Fitting the Pieces of the Liquidity Management Puzzle.” MicroSave Helix Institute of Digital Finance paper.

Korobov Gustav. 2020. “Open Banking as a World of Open Opportunities and Hidden Risks.” Finextra blog post.

KPMG. 2019a. “Consumer Loss Barometer: The Economics of Trust.” Survey.

KPMG. 2019b. “Global Banking Fraud Survey.” Survey.

Kumari Tanwi. 2020. “Client Perspectives on Consumer Protection: Analysis of a Client Survey in Cambodia.” Center for Financial Inclusion Brief.

Levi, Michael, and Russell Smith. 2021. Fraud and Its Relationship to Pandemics and Economic Crises: From Spanish flu to COVID-19. Australian Institute of Criminology research report.

LexisNexis Risk Solutions. “What Is Synthetic Fraud?” LexisNexis article.

RÉFÉRENCES

Mashal, Mujib, and Hari Kumar. 2021. “Using Shame, Lending Apps in India Squeeze Billions Out of the Desperate.” New York Times article.

Masino, Serena, and Miguel Niño-Zarazúa. 2014. “Social Service Delivery and Access to Financial Innovation. The Impact of Oportunidades' Electronic Payment System in Mexico.” World Institute for Development Economics Research Working Paper, Series No. 2014/034.

Maynard, Nick, and Susan Morrow. 2021. “Online Payment Fraud: Emerging Threats, Segment Analysis, Market Forecasts – 2021–2025.” Juniper research.

Mazer, Rafe, and Dan Onchieku. 2019. “Did You See My Tweet: Monitoring Financial Consumer Protection Via Social Media.” FSD Kenya.

Mazer, Rafe, and Kate McKee. 2017. “Consumer Protection in Digital Credit.” CGAP Focus Note.

Mazer, Rafe. 2016. “Interactive SMS Drives Digital Savings and Borrowing in Tanzania.” CGAP blog post.

Mazer, Rafe. 2018. “Kenya's Rules on Mobile Money Price Transparency Are Paying Off.” CGAP blog post.

McKee, Katharine, Michelle Kaffenberger, and Jamie M. Zimmerman. 2015. “Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks.” CGAP Focus Note.

Medine David. 2020. “Financial Scams Rise as Coronavirus Hits Developing Countries.” CGAP Blog Series: Coronavirus (COVID-19): Financial Services in the Global Response.

Medine, David, and Gayatri Murthy. 2020. “https://www.cgap.org/research/publication/making-data-work-poor.” CGAP Focus Note.

Medine, David. 2017. “India Stack: Major Potential but Mind the Risks.” CGAP blog post.

Mehrotra, Aakash, Akhand Tiwari, Karthick Morchan, Mimansa Khanna, and Vivek Khanna. 2018. “State of the Agent Network, India 2017.” MicroSave Helix Institute of Digital Finance, India Country Report.

Mierzwinski, Ed, Teresa Murray, and Mike Litt. 2021. “Virtual Wallets, Real Complaints: How Digital Payment Apps Put Consumers' Cash At Risk – An Analysis of CFPB Complaints.” U.S. PIRG Education Fund Report.

Mishra, Saurabh, Jack Clark, and C. Raymond Perrault. 2020. “Measurement in AI Policy: Opportunities and Challenges.” Research report.

Mohammad, Ghiyazuddin, and Alfa Pelupessy. 2017. “Emerging Risks and Customer Protection in Digital Financial Services in Indonesia.” MicroSave research.

Mondato. 2019. “The Inclusion Illusion: Financial Health In Kenya.” Blog post.

Mondato. 2019. “The Inclusion Illusion: Financial Health In Kenya.” Blog post.

Mondato. 2021. “Digital Lending's Self-regulation: A Redemption Story?” Blog post.

Mukharji, Arunoday. 2021. “The 'Saviour' Loan Apps That Trapped Pandemic-struck Indians.” BBC article.

Munyegera, Ggombe Kasim, and Tomoya Matsumoto. 2017. “ICT for Financial Access: Mobile Money and the Financial Behavior of Rural Households in Uganda.” Review of Development Economics article.

Mureithi, Carlos. 2021. “Inside Africa's Biggest Cryptocurrency Scams.” Quartz Africa article.

RÉFÉRENCES

Mustafa, Zeituna, Mercy Wachira, Vera Bersudskaya, William Nanjero, and Graham A.N. Wright. 2017. “Where Credit Is Due: Customer Experience of Digital Credit in Kenya.” MicroSave report.

Mustafa, Zeituna, Mercy Wachira, Vera Bersudskaya, William Nanjero, and Graham A.N. Wright. 2017. “Where Credit is Due Customer Experience of Digital Credit in Kenya.” MicroSave.

Ndauti, Hildah. 2018. “Cyber Security in Emerging Financial Markets.” CGAP FinDev Gateway publication.

Niño, Jonas Lopez, Jan Langthaler, Marcos Fabian, and Joaquin Mayorga. 2017. “An Overview of FinTechs: Their Benefits and Risks.” Association of Supervisors of Banks of the Americas.

OECD. 2017. “G20/OECD INFE Report: Ensuring Financial Education and Consumer Protection for All in the Digital Age.” Rapport.

OECD. 2019. "Good Practice Guide on Consumer Data." OECD Digital Economy Paper No. 290.

OECD. 2020a. “Personal Data Use in Financial Services and the Role of Financial Education: A Consumer- Centric Analysis.” Rapport.

OECD. 2020a. “Personal Data Use in Financial Services and the Role of Financial Education: A Consumer- Centric Analysis.”

OECD. 2020b. “The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector.” Rapport.

OECD. 2020b. “The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector.”

OECD. 2020c. “Financial Consumer Protection Policy Approaches in the Digital Age: Protecting Consumers' Assets, Data, and Privacy.”

Outseer. 2021. “Outseer Fraud and Payments Report: Digital Transaction Insights from the Outseer Global Data Network,” Q2 2021.

Owens, John. 2018. “Responsible Digital Credit: What Does Responsible digital Credit Look Like?” Center for Financial Inclusion.

Palepu, Advait. 2021. “Troves of Data Stolen by Fake Digital Lending Apps.” Menianama article.

Parkin, Benjamin, and Mercedes Ruehl. 2021. “Asian Authorities Clamp Down on Digital Lenders.” Financial Times article.

Pazarbasioglu, Ceyla, Alfonso Garcia Mora, Mahesh Uttamchandani, Harish Natarajan, Erik Feyen, and Mathew Saal. 2020. “Digital Financial Services.” World Bank Group report.

Political Economy Research Centre. 2015. “Financial Melancholia – Mental Health and Indebtedness.” Rapport.

Prabhakar, Tarunima. 2020. “A New Era for Credit Scoring: Financial Inclusion, Data Security, and Privacy Protection in the Age of Digital Lending.” UC Berkeley Centre for Long-term Cybersecurity.

Prakarsa Policy Brief. 2020. “The Risk of Over-indebtedness Amid COVID-19 Pandemic.”

RÉFÉRENCES

Prakarsa. 2020. “The Risk of Over-indebtedness Amid COVID-19 Pandemic.” Policy brief.

Priezkalns, Eric. 2021. “Are SIM Swaps Rising? Freedom of Information Disclosure Shows UK Police Figures Are Unreliable.” CommsRisk blog post.

Ramanathan, Arundhati. 2021. “India's Instant Loan App Crisis Is Made in China.” The Ken article.

Reaves, Bradley, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin R.B. Butler. 2015. “Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications.” University of Florida paper.

Reitzug, Fabian, Richard Chamboko, Xavier Gine, and Bob Cull. 2020. “Does Agent Gender Matter for Women's Financial Inclusion?” World Bank blog post.

Reserve Bank of India. 2020. “Banking Ombudsman Scheme, 2006, Ombudsman Scheme for NBFCs, 2018, and Ombudsman Scheme for Digital Transactions, 2019: Annual Report - July 1, 2020 to March 31, 2021.” Annual Report. Annual Report.

Responsible Finance Forum. 2017. “Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy.”

Responsible Finance Forum. 2020. “Preventing Over-Indebtedness in Digital Credit Markets: Investors' Checklist.” Discussion Paper Investor Guideline 9: Prevent Over-Indebtedness, Strengthen Digital Literacy and Financial Awareness Prepared by Incofin Investment Management April 2020. Draft Working Paper for Comments.

Responsible Practices Working Group. 2020. “Responsible Practices to Address Seven Major Risks in COVID-19 Digital Financial Transfers.” COVID-19 Global Situation Room convened by the Bill & Melinda Gates Foundation.

Riley, Emma. 2019. “Hiding Loans in the Household Using Mobile Money: Experimental Evidence on Microenterprise Investment in Uganda.” Oxford University Economics Department paper.

Risk Based Security. 2020. “2020 Year End Report.”

Rizzi Alexandra, Isabelle Barrès, and Elisabeth Rhyne. 2017. “Tiny Loans, Big Questions: Client Protection in Mobile Consumer Credit.” Center for Financial Inclusion.

Rizzi, Alexandra, Alexandra Kessler, and Jacobo Menajovsky. 2021. “The Stories Algorithms Tell: Bias and Financial Inclusion at the Data Margins.” Center for Financial Inclusion paper.

Robinson, Jonathan, and Pascaline Dupas. “Knowledge, Use, and Repayment of Digital Credit in Malawi.” Centre for Effective Global Action research.

Rodriguez, Christian, Julia Conrad, Gisela Davico, Susie Lonie, and Lesley Denyes. 2019. “A New Banking Model for Africa: Lessons on Digitization from Four Years of Operations.” IFC report.

Rowntree Oliver. 2019. “The Mobile Gender Gap Report 2019.” GSMA.

RSA. 2018. “RSA Quarterly Fraud Report, Q1 2018.”

RSA. 2020. “Quarterly Fraud Report, Q3 2020.”

Ryan, Chris. 2021. “Solving the Fraud Problem: What is Account Takeover Fraud?” Experian blog post.

SABRIC. “Annual Crime Stats 2018: Contact Crime, Digital Crime, Card Fraud.”

SABRIC. “Annual Crime Stats 2019: Contact Crime, Digital Crime, Card Fraud.”

RÉFÉRENCES

Sahay, Ratna, Ulric Eriksson von Allmen, Amina Lahreche, Purva Khera, Sumiko Ogawa, Majid Bazarbash, and Kimberly Beaton. 2020. "The Promise of Fintech : Financial Inclusion in the Post COVID-19 Era." IMF Departmental Paper No. 20/09.

Sambasivan, Nithya, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Gaytan-Lugo, David Nemer, Elie Bursztein, and Sunny Consolvo. 2019. "'They Don't Leave Us Alone Anywhere We Go': Gender and Digital Abuse in South Asia." Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow.

Sane, Renuka, Srishti Sharma, and Karthik Suresh. 2021. "Grievance Redress in the Financial Sector in India: Lessons from the Field." The Leap Journal blog post.

Schwartz, Leo, and Lucia Cholakian Herrera. 2020. "'Feminist' Ponzi Schemes Are Sweeping through Argentina." Rest of World article.

Serianu. 2017. "Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line."

Serianu. 2018. "Africa Cyber Security Report, Botswana: Cyber Security Skills Gap."

Serianu. 2018. "Africa Cyber Security Report, Kenya: Cyber Security Skills Gap."

Serianu. 2018. "Africa Cyber Security Report, Lesotho: Cyber Security Skills Gap."

Serianu. 2020. "Africa Cybersecurity Report Kenya, 2019/2020: Local Perspective on Data Protection and Privacy Laws – Insights from African SMEs."

Serianu. 2020. "Africa Cybersecurity Report Uganda, 2019/2020: Local Perspective on Data Protection and Privacy Laws – Insights from African SMEs."

Sift. 2020. "Q3 2020 Digital Trust and Safety Index: Account Takeover Fraud and the Growing Burden on Business."

Simmons, Dan. 2017. "BBC Fools HSBC Voice Recognition Security System." BBC Click investigation.

Singh, Arti. 2021a. "A New Worry for Fintech Lenders." The Morning Context article.

Singh, Arti. 2021b. "Inside the Scramble to Cut Off Chinese Loan Apps ." The Morning Context article.

Sivalingam, Isvary, Olivia, Evelyne Matibe, Rahul Chatterjee, Karthick Morchan, Anup Singh, and Leonard Kambona. 2019. "Making Digital Credit Truly Responsible: Insights from Analysis of Digital Credit in Kenya." SPTF, MSC, and the Smart Campaign.

Solli, Jami Hubbard. 2019. "An Intro to UDIS and the MMM Cooperation." Financial Inclusion Global Initiative report.

Spencer, Shelley, Mandana Nakhai, and Jordan Weinstock. 2018. "The Role of Trust in Increasing Women's Access to Finance through Digital Technologies." USAID.

Statista. 2020. "Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025."

Statista. 2021. "Number of Social Network Users Worldwide from 2017 to 2025 (in Billions)."

Stolba, Stephan Lembo. 2020. "How Can Biometrics Protect Your Identity?" Experian blog post.

RÉFÉRENCES

Suryono, Ryan, Indra Budi, and Betty Purwandari. 2020. "Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review."

Theis, Sophie, Giudy Rusconi, Elwyn Panggabean, and Sonja Kelly. 2020. "Delivering on the Potential of Digitized G2P: Driving Women's Financial Inclusion and Empowerment through Indonesia's Program Keluarga Harapan (PKH)." Women's World Banking research.

Toronto Centre. 2018. "Advancing Women's Digital Financial Inclusion." Practical Leadership and Guidance from Toronto Centre. TC Notes.

Totolo, Edoardo. 2018. "Kenya's Digital Credit Revolution Five Years On." FSD Kenya report.

Traynor, Patrick. 2018. "Digital Finance and Data Security: How Private and Secure Data Is Used in Digital Finance?" Center for Financial Inclusion.

UK Finance. 2020. "Fraud – The Facts 2020: The Definitive Overview of Payment Industry Fraud."

Unnikrishnan, Shalini, Jim Larson, Boriwat Pinpradab, and Rachel Brown. 2019. "How Mobile Money Agents Can Expand Financial Inclusion." Boston Consulting Group research.

UNSGSA. 2021. "Financial Service Providers and Financial Health." UNSGSA Working Group on Financial Health report.

Vidal, Maria Fernandez, and Fernando Barbon. 2018. "Digital Credit Helping to Put Kids in Classrooms in Cote d'Ivoire." CGAP blog post.

Waldron, Daniel, and Alexander Sotiriou. 2019." Digital Finance for the Real Economy: Introduction." CGAP slide deck.

Wamalwa, Peter, Ireen Rugiri, and Julienne Lauler. 2019. "Digital Credit, Financial Literacy, and Household Indebtedness." KBA Centre for Research on Financial Markets and Policy Working Paper.

Warburton David. 2020. "Phishing and Fraud Report: Phishing During a Pandemic." F5 Labs.

Wechsler, Michael, and Samikshya Siwakoti. 2020. "Gender, Cybersecurity and Fraud in DFS." Columbia University Digital Financial Services Observatory.

Wein, Tom, Mercy Musya, Rafe Mazer, and Maria Fernandez Vidal. 2017. "Do Peer-to-Peer Lenders Understand Risk?" CGAP bog post.

White, Zachary. 2020. "VITALITE Zambia: Learnings from Providing Pay-as-You-Go Smartphones through Pay-as-You-Go Solar." GSMA Mobile for Development blog post.

World Bank DataBank. "Mobile Cellular Subscriptions – South Africa."

Banque mondiale. 2019. "Complaints Handling within Financial Service Providers Principles, Practices, and Regulatory Approaches." World Bank Group Technical Note.

Banque mondiale. 2021. "Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches." Policy Research Paper.

Wright, Graham A.N. 2015. "A Question of Trust Mitigating Customer Risk in Digital Financial Services." MicroSave.

RÉFÉRENCES

Wright, Graham, and Vera Bersudskaya. 2017. “More Than Hygiene – Improving Agent Network Performance to Maximise Profitability.” Microsave Consulting ” Helix Institute of Digital Finance. blog post.

Wright, Graham, Nitish Narain, and Manoj Nayak. 2018. “Consumer Protection in the Digital Age.” MSC blog post.

Zetterli, Peter. 2013. “Can Phones Drive Insurance Markets? Initial Results from Ghana.” CGAP blog post.

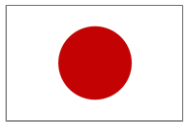
Zhang, Daniel et al. 2021. “The AI Index 2021 Annual Report.” AI Index Steering Committee, Human-Centered AI Institute, Stanford University.

Zhang, Shu, and Ryan Woo. 2017. “After Spate of Suicides, China Targets Predatory Student Lending.” Reuters article.

Zimmerman, Jamie, and Silvia Baur-Yazbeck. 2016. “Understanding Consumer Risks in Digital Social Payments.” CGAP Brief.

CGAP

www.cgap.org



MEMBRES DU CGAP AU MOIS DE JANVIER 2022

CGAP

CGAP.ORG