

FICHIER NON ÉDITÉ COMPLÉTÉ

Webinaire # 10 - Les exigences d'interopérabilité et de résilience  
des services financiers numériques

UIT -- Genève

27 JUILLET 2020, 15 h 30

Services rendus par :

Caption First, Inc.

P.O. Box 3066.

Monument, CO 80132.

1 877 825 5234.

+001 719 481 9835.

[www.captionfirst.com](http://www.captionfirst.com) <<http://www.captionfirst.com>>

\*\*\*

Ce texte, document ou fichier est basé sur la transcription en direct. La communication en temps réel (CART), le sous-titrage et/ou la transcription en direct sont fournis afin de faciliter l'accès à la communication et peuvent ne pas être un compte rendu complet des débats.

\*\*\*

**>>BILEL JAMOUSSEI** : Bonjour, bon après-midi, bonsoir et bienvenue au dixième épisode de la série de webinaires en temps de COVID-19 organisés par l'UIT. Nous espérons que vous, votre famille, vos amis et vos collègues êtes tous en bonne santé et en sécurité.

Je m'appelle Bilel Jamoussi, chef du département des commissions d'étude au Bureau de normalisation de l'UIT à Genève et c'est un privilège pour moi de présenter le webinaire d'aujourd'hui sur les exigences d'interopérabilité et de résilience des services financiers numériques.

Avant de présenter les panélistes, je fournirai des informations générales sur la logistique du webinaire d'aujourd'hui. Nous avons quelques participants connectés de différents pays. Toutes les

présentations seront disponibles après le webinaire sur le site Web de l'événement. Je suis heureux d'annoncer que nous avons le sous-titrage en français. Toutes les questions des participants seront prises à la fin de toutes les présentations, lors de la session de questions et réponses. Les participants peuvent soumettre leurs questions en les tapant dans la fenêtre Q&R. Lors de la soumission d'une question via la fenêtre Q&R, j'invite le participant à saisir d'abord le nom du panéliste à qui la question est adressée suivi de la question. Si la question est adressée au panel en général, veuillez saisir votre question directement sans le nom du panéliste. Les intervenants vont parler dans l'ordre suivant : Dorothee Delort de la Banque mondiale, Kevin Butler d'Université de Floride, Monsieur Anant Nautiyal de GSMA, Monsieur Saleh Khan de l'UPU et Monsieur Abhinav Pratap Singh du Département des postes du Gouvernement indien.

Nous allons étudier les problèmes d'interopérabilité et de résilience dans les économies en émergence et l'impact pendant la COVID-19. L'interopérabilité est un travail crucial pour les infrastructures financières et informatiques pour mettre les services financiers numériques à disposition de façon généralisée.

Pour les personnes qui ont accès aux services financiers et à l'interopérabilité des paiements, cela permet à ces personnes de transférer leur argent à d'autres individus sans avoir à recourir à des comptes de transactions multiples. Un nombre de recommandations ont été émises. Par exemple, les autorités et le fournisseur fournissent une interopérabilité par l'engagement avec les fournisseurs de services financiers numériques. Les autorités financières peuvent prendre la direction de l'interopérabilité des services financiers numériques et d'autres parties prenantes clés. On travaille à l'implantation de l'interopérabilité et les autorités financières doivent clarifier le rôle des parties prenantes publiques et privées y compris les parties prenantes dans le processus. Les fournisseurs de services financiers numériques devront prendre

responsabilité et identifier et atténuer les risques en question pour s'assurer que la responsabilité pour l'atténuation des risques est adressée de façon correcte. Dans les épisodes précédents des webinaires, les problèmes de crimes cybernétiques et d'escroquerie ont été soulignés et les fournisseurs doivent prendre les étapes nécessaires pour améliorer les capacités de résilience avec l'objectif de limiter les risques en croissance des menaces cybernétiques. Dans ce contexte, la résilience ou l'infrastructure des paiements numériques pour anticiper, résister et se remettre rapidement d'une attaque est très complexe et critique dû au rôle et à l'interdépendance des parties prenantes pour l'écosystème et pour le système écosystème de paiement mobile; il s'agit en effet d'un écosystème très complexe. Ces menaces et ces risques doivent être gérés de façon soigneuse pour minimiser l'impact sur la stabilité du système de paiement. Le niveau de résistance peut être un facteur décisif dans la résilience générale du système financier et de l'économie en général.

Selon l'initiative mondiale de l'inclusion financière et l'infrastructure de sécurité dirigée par l'UIT, on a développé un cadre d'assurance de sécurité des services financiers numériques et des mesures ont été identifiées de vulnérabilité et des menaces au niveau de l'infrastructure du réseau et des applications à ce sujet. Le travail de la sécurité cybernétique mené par la Banque mondiale avec la Banque centrale européenne pour concrétiser les initiatives sur la résistance cybernétique pour se conformer avec les directives des autorités pour évaluer les FMI et améliorer de ce fait la résilience qui est critique à la stabilité financière et à l'inclusion financière.

Nous nous trouvons maintenant vers nos intervenants et je vais les inviter à faire leur présentation chacun pour 15 minutes. Notre premier intervenant est Madame Dorothee Delort de la Banque mondiale. Vous avez 15 minutes.

**>>DOROTHÉE DELORT** : Merci beaucoup, Bilel. Bonjour, bonsoir, Mesdames et Messieurs. Je suis heureuse de vous parler aujourd'hui au

sujet de l'interopérabilité et la résilience pour le système de paiement numérique. La Banque mondiale travaille beaucoup sur les fondations critiques pour les paiements numériques et l'inclusion financière. Dû à ses fondations critiques elles vont nous permettre de bâtir un écosystème financier solide. L'objectif que nous poursuivons dans notre travail sur cette fondation sera sécurité et l'efficacité du système de paiement international. La sécurité a affaire à la résilience, bien sûr, et l'efficacité et l'interopérabilité est très critique. Pour travailler à cela et pour établir ces fondations et pour les paiements numériques, nous travaillons au cadre juridique, à l'infrastructure technique et les politiques publiques et les engagements du secteur privé. Sur la base de ces fondations, nous pouvons bâtir des piliers comme les comptes d'action et les produits de paiement et des points d'action pour la numérisation. Tout cela dans le cadre des objectifs de l'accès universel aux comptes de transaction et à leur usage fréquent. Comment est-ce que la Banque mondiale travaille à ces fondations critiques? Nous le faisons avec beaucoup d'outils qui vont jusqu'aux données analytiques. Nous pouvons parler de la technologie financière mondiale. Nous le faisons au niveau du pays. Nous faisons des stratégies de paiement et des stratégies de paiement numérique, des stratégies de technologie financière et par le biais de notre rôle par lequel nous finançons les infrastructures critiques ou les changements nécessaires pour établir des systèmes de paiement sécuritaires et stables. Prochaine diapositive, s'il vous plaît.

Notre travail porte aussi sur un nombre de produits technologiques et d'accès. Maintenant, quand nous travaillons sur l'interopérabilité et la résilience pour les systèmes de paiement nationaux pour l'infrastructure des pays financés il faut toujours prendre en compte l'innovation dans le domaine des paiements et ces innovations peuvent avoir un impact sur nos produits. C'est le cas pour les devises de la Banque mondiale, les paiements instantanés et les portefeuilles

électroniques. Ces technologies ont un impact sur les technologies sous-jacentes comme la biométrie, la technologie sans contact, et cetera. Tous ces changements aux produits et aux technologies, aux modes d'accès doivent être pris en compte quand nous travaillons sur le diagnostic et les recommandations pour le système national où l'inclusion financière et les stratégies reliées. Prochaine diapositive.

Pour atteindre ces buts, pour que ce soit sécuritaire, inclusif et un système de paiement inclusif et soutenu par des initiatives de marché financier sécuritaires nous nous servons des normes développées par des entités officielles et des comités semblables pour la sécurité et le système de sécurité. Ces principes pour les infrastructures des marchés financiers peuvent être catégorisés en neuf catégories larges. Elles comprennent un nombre de considérations et de recommandations clé pour pouvoir améliorer l'organisation générale telle que la gouvernance, la gestion des risques. Elles comprennent aussi des recommandations spécifiques pour les risques des crédits et les risques de liquidités pour les risques liés aux règlements et, très important, les risques liés à l'accès, à l'efficacité et la transparence.

Prochaine diapositive.

Ces principes, l'infrastructure des marchés financiers comprend des recommandations clés qui vont soutenir l'interopérabilité. L'interopérabilité doit être basée sur le cadre juridique et la réglementation des systèmes pour avoir des fournisseurs de paiement non bancaires. Il faut avoir un cadre juridique qui va permettre des fournisseurs de paiement non bancaires à exister sur le marché qui va mettre en place le règlement pour les lois et pour la gestion et la surveillance de ces fournisseurs de services de paiement non bancaires. On doit leur donner accès à une infrastructure critique pour pouvoir favoriser l'interopérabilité et pour cela nous avons des recommandations dans les principes 18, 19 et 20. C'est aussi clé que la gouvernance de l'infrastructure des marchés financiers prenne en

considération le besoin de toutes les parties prenantes et cela va beaucoup contribuer à l'interopérabilité. Nous voyons que dans beaucoup de pays l'interopérabilité ne va pas être obtenue parce que les parties prenantes ne sont pas vraiment représentées de façon adéquate dans l'infrastructure des marchés financiers. La Banque mondiale a aussi un rôle important à jouer et un des rôles implique la création des conditions pour la coopération et le dialogue avec les parties prenantes surtout sur la question de l'interopérabilité.

Prochaine diapositive.

En ce qui concerne la résilience, j'aimerais insister sur le fait qu'il y a plus que simplement une - il ne s'agit pas seulement - la résilience commence par la résilience juridique et sur une base juridique solide. Parce que si on n'a pas une base solide pour les règles juridiques solides pour les règlements et le règlement est mis en question, il n'y a pas de résilience possible pour le marché financier et pour les services de paiement. Il y a aussi ce que j'appellerais une résilience organisationnelle qui a affaire avec la façon dont la gouvernance est organisée et la gestion des risques est organisée. Il y a aussi un niveau de risque de crédit et de risque de liquidités et aussi un risque d'affaires générales. Pour qu'un système de paiement soit résilient, il doit pouvoir gérer ses opérations pendant au moins six mois. Donc, c'est le risque que la résilience d'affaires générales. Mais ce que j'aimerais me concentrer en particulier, c'est la résilience opérationnelle et sur la résilience cybernétique. Prochaine diapositive, s'il vous plaît.

La prochaine.

Alors, pour le risque opérationnel, je vais passer là-dessus très rapidement, mais le Fonds monétaire international comprend des considérations clé pour pouvoir identifier la source possible de risques opérationnels en interne et externe et pour atténuer l'impact des systèmes appropriés et des politiques et des procédures et des contrôles. Les systèmes doivent être créés pour assurer un degré de

sécurité élevé et de fiabilité solide. La gestion de continuité des affaires doit se diriger vers une recouverte ponctuelle des opérations et pour satisfaire aux obligations du Fonds monétaire international y compris dans des événements à grande interruption à large échelle. Nous avons pris des risques dans le cas de la COVID-19, parce qu'il y avait le manque de personnel critique parce que ce personnel critique au niveau des systèmes de paiement et au niveau des participants est susceptible de ne pas être disponible. Donc, la banque centrale et d'autres parties prenantes ont dû prendre des mesures spécifiques pour faire face au risque lié à l'infrastructure dû à la COVID-19. Prochaine diapositive.

Certaines des considérations clé sont très détaillées pour le principe numéro 17 on doit se souvenir que la philosophie n'est pas d'être strict mais de donner de la souplesse aux opérations des systèmes de paiement et sur les objectifs à atteindre. Prochaine diapositive, s'il vous plaît.

J'aimerais maintenant me concentrer plus spécifiquement sur la résilience cybernétique et je trouve que ces graphiques sont très intéressants parce que cela met en perspective les espaces respectifs qui sont au sein de la gestion du risque qui sont occupés par la continuité d'affaires, la sécurité cybernétique et l'informatique.

J'aimerais me concentrer pour l'instant sur la résilience cybernétique simplement un aspect spécifique de l'interopérabilité et qui comprend la sécurité cybernétique. Prochaine diapositive, s'il vous plaît.

La prochaine diapositive, s'il vous plaît.

Le CPMI-IOSCO, l'entité de l'infrastructure financière pour compléter le Fonds monétaire international a donné des directives spécifiques structurées en chapitre qui définissent cinq catégories de gestion des risques principaux qui sont la gouvernance, l'identification, la protection, la détection et le recouvrement. Trois composantes générales sont le test, la conscience de la situation

et l'apprentissage et l'évolution. Ensemble, ils constituent la résilience, la guidance de résilience cybernétique. Le problème, c'est que c'est un peu à haut niveau et nous pensons que dans le cadre du FIGI et la résilience cybernétique il y a besoin d'un outil plus spécifique ou des méthodologies plus spécifique pour mettre en opération ces directives. C'est là que nous avons travaillé avec la Banque centrale européenne qui a développé des attentes de résilience cybernétique pour fournir aux opérations de systèmes et aux autorités, et cetera, des élaborations plus détaillées sur la façon de mettre en place toutes ces directives. On a fourni des directives quand on donne des retours au Fonds monétaire international et ils prennent en considération les meilleures pratiques du secteur qui sont déjà détaillées dans le cadre de la COVID-19 et d'autres cadres. Prochaine diapositive, s'il vous plaît.

Dû au fait que le système et l'infrastructure des marchés financiers sont très différents d'un pays à l'autre ou même au sein d'un même pays avec différent niveau de détail, trois niveaux ont été définis sur la base, sur le niveau de détail des systèmes.

Le niveau de raffinement des systèmes; ce sont les niveaux d'innovation, d'avancement et d'évolution. Prochaine diapositive. Je vais suggérer que vous regardiez au site FIGI, au site de la Banque mondiale, de la Banque centrale européenne, parce que pour chacune des catégories, il y a des suggestions très détaillées et des recommandations pour la gouvernance, pour l'identification, la protection, la détection, la réponse et le recouvrement. Et les tests à ce sujet et ils fournissent un outil très efficace pour améliorer la résilience sur lequel seront bâtis les services financiers numériques. Je vais m'arrêter ici parce que j'ai atteint la fin de mon temps. Merci beaucoup. Je prendrai des questions plus tard.

**>>BILEL JAMOSSI** : Merci beaucoup, Dorothée, d'avoir partagé avec nous des informations importantes pour la sécurité et l'efficacité du paiement, des systèmes de paiement pour favoriser les paiements



numériques et aussi d'avoir souligné le principe 17 des risques d'opération et comment FIGI travaille à aider pour l'implantation de cela. Notre prochain intervenant est Kevin Butler de l'Université de Floride pour 15 minutes.

**>>KEVIN BUTLER** : Merci. Je vais mettre ma présentation à l'écran. Vous pouvez voir mes diapositives?

Je vais parler de l'amélioration dans l'écosystème -

**>>BILEL JAMOSSI** : On ne voit pas tes diapositives, encore.

**>>KEVIN BUTLER** : Merci, Bilel.

**>>BILEL JAMOSSI** : C'est bon.

**>>KEVIN BUTLER** : La COVID-19 a créé des problèmes sans précédent sur l'économie mondiale. On voit des changements au niveau de la vie quotidienne et des services dont on se sert et nous faisons face à des effets à grande échelle. La COVID-19 exacerbe les inégalités. Les services financiers numériques jouent un grand rôle pour maintenir la connectivité et fournir des services valables aux utilisateurs comme les services financiers numériques et dans beaucoup de manières les services financiers numériques sont très bien situés pour gérer la pandémie. Cela signifie que cela atténue le besoin pour le voyage physique et cela accroît la sécurité de ce point de vue. Mais l'écosystème des services financiers numériques est très vulnérable à beaucoup de menace et basé sur trois raisons : l'interconnectivité des entités du système, deuxièmement se fier au nombre de partie et troisièmement l'écosystème même est de plus en plus complexe en ce qui concerne les dispositifs utilisés et les systèmes d'opération qui sont utilisés par ces dispositifs qui deviennent de plus en plus complexes dû aux attaques croissant. Je vais me pencher sur un cadre de sécurité dans le contexte des services financiers numériques. Pourquoi y a-t-il un contexte de sécurité et comment cela a trait à la résilience quand on se penche sur les menaces liées à la COVID-19? Les menaces sont identiques., la résilience c'est la possibilité de résister et de se remettre des difficultés opérationnelles. Donc, la planification de

la continuité, la sécurité, identifier les attaques. Quand on pense à la sécurité, on pense surtout à la protection des systèmes informatiques et les données contre les adversaires. En ce qui concerne la sécurité et les politiques de sécurité qui considèrent seulement la protection, cela ne va pas s'avérer résilient. Si vous avez une politique de sécurité cybernétique c'est bien mais pas nécessairement un cadre de résilience. Mais si vous avez un cadre d'assurance de sécurité qui vous permet d'évaluer le risque et qui vous permet de développer des processus, là vous avez une structure en place qui, du fait d'avoir le moyen de développer des stratégies d'évaluation des risques et des processus pour gérer ce genre de problèmes, vous aurez aussi les bénéfices de développer une résilience en résultat.

Je vais parler du cadre d'assurance de la sécurité qui a été développé dans le cadre de la sécurité mondiale et internationale ou FIGI. Ils veulent lier les carences liées à la connaissance et recommander des méthodologies de structure. Ces buts sont multiples. Par exemple, en ayant un cadre en place, cela permet à l'écosystème DFS d'améliorer la confiance de la clientèle au sein de l'écosystème. Cela permet d'identifier les menaces et les vulnérabilités liées à la sécurité au sein de l'écosystème. Cela établit des contrôles de sécurité et cela permet de rendre les pratiques de gestion plus solide en ce qui concerne le risque de sécurité de façon inclusive pour toutes les parties prenantes. Il y a une adresse du site Web pour le cadre d'assurance des sécurités des services financiers numériques. Vous pouvez l'écrire ou regarder cela plus tard.

Vous allez trouver une copie du cadre de sécurité que je vous encourage à lire quand vous en aurez le temps. Je vais me pencher sur les concepts importants pour que vous puissiez vous et moi tous être d'accord - la vulnérabilité est une faiblesse d'un système qui peut être exploité par un adversaire mais le risque c'est la conséquence de la menace déployée de façon réussie. La recommandation X.805 fournit une fondation pour le document pour faire face à la sécurité pour le

contrôle de l'accès, à l'authentification. Il s'agit d'une vue très générale. Si vous voulez quelque chose de plus détaillé, consultez le document, mais de façon générale les parties importantes de notre point de vue sont l'utilisateur, l'opérateur du réseau et le fournisseur des services financiers numériques. L'utilisateur est l'audience cible qui se sert de l'application mobile d'argent ou sur des dispositifs mobiles et ils se servent d'une application. L'opérateur du réseau fournit une infrastructure de communication sans lien pour le réseau. Et le fournisseur des services financiers numériques gère toutes ces composantes. La façon dont nous évaluons le risque est basée sur le cycle, plan, vérification et agir. Cette idée est sans nous pour établir la résilience. L'objectif de la méthodologie est de surveiller et de réviser et cela dépend des parties prenantes. Par exemple, le régulateur va réviser les contrôles et sur la base des informations les gens en changement peuvent - les changements peuvent être effectués et tous les contextes seront nécessaires pour avoir une évaluation des risques effectifs, évaluation et analyse. Et le cadre standardisé peut être utilisé dans n'importe quel contexte. En résumé, les menaces de l'écosystème - il y a 17 menaces différentes peut-être même plus, mais à un niveau élevé avec le cadre nous avons examiné ces menaces, de la façon dont elles s'appliquent sur les parties prenantes de l'écosystème, les fournisseurs, les utilisateurs, et cetera. Nous avons développé 118 contrôles différents qui pourraient être utilisés en tant que moyen d'évaluer, d'atténuer et de faire face aux menaces. Au fait, sur chacune de ces parties prenantes on voit des exemples de menaces et les chiffres entre parenthèses font référence aux parties du rapport. Un exemple : un déni de services. C'est une menace standardisée que nous considérons dans la section 8,7 du document. Cela peut être caractéristique d'une attaque créée pour empêcher le service dans l'écosystème et les empêcher d'être offert et cela affaire spécifiquement à la résilience parce que le manque de services n'est pas toujours dû à une attaque. Cela peut être dû à une inscription aux

services et certainement pendant la COVID-19, nous avons vu que des fournisseurs de services font l'objet d'utilisateurs supplémentaires pendant un temps trop réduit. Donc, on ne peut même pas distinguer cela d'une attaque réelle. Nous avons examiné dans le contexte DFS, nous avons parlé des fournisseurs de services mobiles. Pour rester ponctuel, je vais parler d'un exemple : le risque de vulnérabilité et de contrôle de la part de l'opérateur du réseau; impossibilité d'effectuer les opérations dues à une interruption du service et d'échec des opérations dû à des retards élevé. La vulnérabilité, c'est dû à l'interruption du réseau dû à l'entretien ou à la création de l'infrastructure. Les contrôles que nous avons identifiés dans le document sont les contrôles 22 et 23. L'opérateur du réseau mobile doit prendre des mesures pour assurer la disponibilité du réseau pour avoir accès aux services financiers numériques et le 23 dit que l'opérateur du réseau mobile doit faire des tests simulant des opérations diverses basées sur le nombre des clients, la croissance à laquelle il s'attend pour continuer à avoir un rendement du système optimal. Le système doit donner un contrôle comme chaque contexte est individuel nous allons dans différents niveaux de détail en fonction des divers membres du système pour permettre aux fournisseurs de services d'établir une structure solide. Dans le cadre d'assurance de la sécurité est créé pour fournir des directives aux parties prenantes au sein de l'écosystème des services de paiement numérique. Il n'est pas fait pour être statique parce qu'un document est vivant et les conseils de sécurité vont évoluer. Surtout en ce qui concerne la résilience, d'une approche systématique pour développer les processus et les contrôles qui sont informés par les menaces et les risques contre l'écosystème des services financiers numériques vont assurer sa résilience. Ce document peut être un moyen d'assurer que votre système et votre infrastructure et votre écosystème sont développés pour être résilients contre les attaques, que ce soient les attaques malveillantes ou les menaces à l'écosystème que nous avons vu en raison de la COVID-19. Je suis heureux

de répondre aux questions dans le futur et j'apprécie d'avoir eu la possibilité de parler aujourd'hui.

**>>BILEL JAMOSSI** : Merci beaucoup, Kevin Butler de l'Université de Floride de nous avoir introduits à ce système et ces trois composantes et nous donner un exemple de certains des contrôles mis en place. Merci de la référence à 805 et les dimensions de la sécurité. Le cadre de sécurité est très important pour assurer la résilience aux fournisseurs de services. Nous allons revenir vers toi pendant la période des Q&R. Je passe maintenant à notre prochain intervenant, Anant.

**>>ANANT NAUTIYAL** : Merci beaucoup, Bilel. Je vais partager mon écran. Voilà. Vous voyez?

**>>BILEL JAMOSSI** : Oui, c'est bon. Allez-y.

**>>ANANT NAUTIYAL** : Très bien. Merci à nouveau de m'avoir donné l'occasion de présenter aujourd'hui. Je vais faire une petite introduction en ce qui concerne le GSMA; c'est l'association d'opérateurs mondiaux et je travaille dans l'équipe d'interopérabilité de l'argent et cela comprend un laboratoire technique. Dans le contexte dans lequel nous nous sommes impliqués dans ce sujet, voici la première diapositive. Cela fournit une inclusion monétaire. Aujourd'hui, à l'heure actuelle, nous avons plus d'un milliard de comptes d'argent mobile enregistrés. Le rapport, c'est dû dans certains marchés les fournisseurs de services ont donné accès à l'argent mobile. Dans d'autres marchés, le gouvernement a pris un rôle plus grand dans ce sujet et dans d'autres endroits les projets numériques sont en train de se bâtir pour bâtir des services monétaires interconnectés. Le lancement des paiements, des systèmes numériques, sont très importants pour la façon dont l'interopérabilité peut être faite. Pour les fournisseurs de paiement numérique dans les marchés en émergence, et aussi les fournisseurs non bancaires, cela peut être un choix très difficile à faire parce que le marché technique pour l'interopérabilité nous collaborons avec beaucoup de gens qui demandent de quoi il s'agit.

C'est la raison pour laquelle nous avons émis un rapport récent et vous l'avez sur votre écran à gauche. Cela s'appelle les diverses façons - les différents moyens d'interopérabilité de l'argent mobile. La connexion avec ce travail est le sujet de la discussion d'aujourd'hui, c'est qu'un des facteurs que nous avons identifié dans ce rapport, à la fin, comme je vais vous le dire, c'est la résilience de l'interopérabilité. Nous appelons cela dans notre rapport la solidité. Donc, la première raison, ces deux sujets se touchent parce que la résilience est très importante pour les solutions financières. Pour en revenir au rapport, nous avons adopté une méthode très simple sur la question de savoir quel est le meilleur modèle. Nous définissons cinq composantes que nous pensons la fondation des solutions. Elles sont sur l'écran : la connexion, la gouvernance, le modèle de tarification, le règlement et le mécanisme de résolution des différends. C'est la meilleure façon que nous avons trouvée pour définir les éléments fondamentaux. Les participants peuvent comprendre tout cela.

Le règlement a affaire aux mécanismes de règlement qui permet le flux de l'argent réel et la gouvernance réfère à la façon dont les participants sur les solutions d'interopérabilité prennent leurs décisions. Le modèle de tarification et d'affaires comprend les déterminants clé d'une interopérabilité et finalement les mécanismes de règlement des différends. Ces cinq composantes pour les solutions d'interopérabilité, vous avez sous chacune des composantes des caractéristiques assez générales. Ce sont les caractéristiques de base; sous connexion, vous avez la connexion bilatérale. Vous avez peut-être un site centralisé. Pour le règlement, nous avons sur une base qui précède les fonds, ou avant l'opération, où vous pouvez faire le règlement après l'opération et cela s'appelle sur la base de la liquidation. Vous pouvez avoir un contrôle complet ou un contrôle partiel en ce qui concerne la gouvernance. Vous avez au niveau du modèle d'affaires et des tarifications vous avez les frais de traitement,

l'interchangement et en ce qui concerne le règlement des différends vous avez le consensus ou l'arbitrage. Toutes ces composantes ne sont pas dépendantes; elles sont interdépendantes. Sous la gouvernance les participants, par définition, n'ont pas de contrôle. Pour l'option d'un certain contrôle, cela va avoir une influence sur les autres.

Je vais montrer ici ce qui se passe quand vous mettez ensemble certaines options et vous les mettez les unes avec les autres. Vous obtenez des scénarios divers et vous voyez quatre modèles possibles pour obtenir et faire que toutes ces composantes soient interopérables. Vous pouvez avoir un modèle d'accord bilatéral; troisièmement un modèle d'argent mobile et quatrièmement c'est un système mondial. C'est au niveau d'un concentrateur. Tous ces modèles ont une infrastructure distincte. Vous voyez sur cette diapositive, vous pouvez regarder après la présentation, mais à gauche, en gros, vous avez les diagrammes techniques. Il y a le modèle bilatéral, le modèle agrégation et le modèle du concentrateur. L'architecture de l'impact en ce qui concerne au niveau technique et aussi commercial. Sur l'écran, vous voyez en haut le côté technique, l'impact sur la création et les protocoles d'identification des comptes et si les clients se servent des dollars américains, du point de vue de l'interruption du système quelles sont les chances de revenir, cela touche à la résilience et du côté commercial vous avez CAPEX et OPEX, combien de temps vous avez pour les dynamiques et les autres parties prenantes et les temps d'intégration. Il s'agit simplement ici d'un résumé de ce qui se passe. Finalement, en menant à la fin de l'analyse, nous allons nous servir d'une évaluation à haut niveau des modèles d'interopérabilité que nous avons inclus dans notre rapport. Quelles sont les forces et faiblesses de ces divers modèles. Vous avez en grandes lettres à droite, il n'y a pas de bonne réponse, tous les modèles ont leurs forces et leurs faiblesses. Je veux simplement fournir aux fournisseurs de paiement un genre de boîte d'outils pour évaluer dans le cadre de leurs propres décisions et pour savoir dans quelle direction

ils se dirigent. Nous avons mentionné qu'en général pour la position du GSMA sur l'interopérabilité il y a une priorité stratégique pour les fournisseurs d'argent mobile. Mais pour la durabilité à long terme, il faut que ce soit dirigé par le marché. Voici le résumé de ce qui se passe. Je suis content d'avoir pu partager ma recherche avec vous, quoiqu'il s'agisse là d'une analyse à haut niveau, n'hésitez pas à me poser n'importe quelle question. Si vous voulez examiner ce rapport plus en détail, nous le tenons à votre disposition. Je vais m'arrêter.

**>>BILEL JAMOSSI** : Merci, Anant, d'avoir partagé avec nous l'interopérabilité. Tu as mentionné le règlement, le règlement des différends et les différentes options pour faire face à tous ces problèmes. Je me suis souvenu des chiffres très intéressants de 179 fournisseurs de services mobiles au niveau mondial et les milliards de dollars d'argent en circulation et les 2 millions de chiffres traités par jour. Vraiment, cela indique que c'est à une échelle mondiale très élevée -

**>>ANANT NAUTIYAL** : Je me suis trompé, c'est en fait 299 fournisseurs mobiles. Je me suis trompé.

**>>BILEL JAMOSSI** : Merci de cette correction. Je passe maintenant à Monsieur Saleh Khan.

**>>SALEH KHAN** : Merci. Je vais partager mon écran. Je veux introduire ce sujet très rapidement et les sondages au niveau mondial. Il y a plus d'un milliard de personnes au niveau mondial qui fournit ce grand réseau dans le monde. Pendant la pandémie de COVID-19, on fournit des services et partout dans le monde et il s'agit là de services essentiels. Et les personnes forcées de rester chez eux, cela leur permet d'avoir des services financiers numériques chez eux en ligne. Tirant parti d'une relation de confiance avec la communauté ils deviennent des partenaires évidents pour la gouvernance partout dans le monde. Il y a des exemples de cela dans notre site Web. Vous pouvez y aller et nous remarquons que les pensions sont livrées, le liquide est livré. Il y a ici un mécanisme en place pour les personnes chez



eux. Je vais parler et Monsieur Abhinav Pratap Singh va l'expliquer plus en détail; il travaille au Département des postes.

**>>ABHINAV PRATAP SINGH** : Merci, bonjour, bonsoir à tout le monde. Je vais partager ma vidéo. Voyez-vous l'écran?

**>>BILEL JAMOUSSE** : Oui.

**>>ABHINAV PRATAP SINGH** : Merci de cette opportunité de présenter le système de paiement de l'Inde qui est de l'interopérabilité. Comme on l'a mentionné, pendant la COVID-19, ce sont des prestataires de services essentiels et ils peuvent travailler dans ce contexte sans précédent. Ma présentation comprend l'inclusion financière de l'Inde, l'infrastructure pour le bien public et comment cela a mené beaucoup de personnes qui sinon auraient été laissées en dehors de l'inclusion financière et comment le Département des postes du Gouvernement indien a travaillé dans le cadre de ce système et comment nous avons travaillé dans le système de paiement. Comme Saleh Khan l'a mentionné, le réseau comprend 1,96 milliard de comptes, des transferts d'argent, des paiements. Seulement 8 % de postes offrent un éventail agrandi de produits et de prestations. L'inclusion financière est un objectif de développement important parce qu'il y a une grande corrélation entre les comptes bancaires et le nombre d'habitants. L'objectif de l'inclusion financière c'est d'être inclus dans les objectifs des Nations Unies, même avec l'amélioration de la technologie financière il y a quand même des milliards de personnes exclues et beaucoup d'entre elles sont des femmes. Il y a beaucoup d'inégalité entre les sexes en ce qui concerne l'inclusion financière et nous voulons inclure ces personnes dans le réseau postal financier. La façon dont nous pouvons atténuer les défis d'accessibilité pour atteindre le but d'inclusion financière. La poste indienne est très ancienne; nous avons 360 millions de comptes d'épargne. La poste indienne fournit beaucoup de services. Il y a presque trois billions de roupies; il faut avoir une technologie de paiement en place et la poste de l'Inde a fait une demande de licence que nous avons obtenue et maintenant nous avons une

nouvelle entité. Les régulateurs, s'ils avaient pris cela de façon conventionnelle ils auraient mis 47 ans à obtenir leur but. Presque tous les Indiens ont des comptes. Pour avoir atteint l'inclusion financière - nous avons ces services au niveau rural et nous avons pour les personnes dans les régions rurales, il y a presque - cela a permis à 3 millions de personnes d'ouvrir un compte bancaire. Cela a créé des catégories de banques différenciées et des correspondants bancaires qui ont été établis dans cette catégorie. Troisièmement, cela permet aux banques d'avoir - pour avoir pas seulement des - ils peuvent être gérés avec des banques multiples. C'était une numérisation très importante de la population indienne. Maintenant, nous avons plus d'un milliard d'utilisateurs de téléphone mobile. En décembre 2020, nous aurons plus de 6 millions d'utilisateurs. Cela permettra l'inclusion financière de pénétrer les régions rurales. C'était un élément critique pour ouvrir un compte bancaire et pour pénétrer dans le système financier. Le Gouvernement indien a compris le programme biométrique le programme le plus large. C'est un programme d'identification et de ce point de vue depuis 2008, nous avons des milliards de citoyens qui ont une identité numérique. Cela a permis à beaucoup d'autres produits d'être développés en plus de cette innovation qui a permis l'inclusion financière de se faire passer de façon élargie. Le Gouvernement indien a commencé d'autres initiatives pour bâtir les capacités en ce qui concerne fournir des machines de points de vente et d'autres infrastructures. En ce qui concerne les innovations de technologie financière qui jouent un grand rôle, il s'agit de différentes compagnies et il y a beaucoup de comptes bancaires et des mécanismes d'authenticité, cela a été crucial pour la structure financière en Inde. Pour permettre à la population de l'Inde qui a la plus grande population du monde. Les paiements du gouvernement aux individus ont été authentifiés de façon améliorée et cela a eu un grand bénéfice pour nous pour permettre les paiements des gouvernements qui peuvent être versés dans des comptes individuels directement. En ce qui concerne

India Stack, c'est un système de paiement résilient. La plupart étaient avant de pair à pair. Il y avait une boucle de paiement fermé. Grâce au programme maintenant, c'est ouvert et cela fait preuve d'interopérabilité. C'est caractérisé par l'interopérabilité. Chaque niveau et plateforme ont été créés pour gérer le système de paiement. Comme Dorothee l'a dit, ces systèmes de paiement font l'objet de beaucoup de régulations de paiement pour être résilient et cela a été créé dans le cadre régulateur et combiné avec des produits à bon marché.

Le premier niveau c'est le niveau de consentement par le biais du programme que j'ai mentionné dans la diapositive précédente. Pas besoin de la présence physique de la personne. Cela a permis de baisser les coûts connexes. Comme je l'ai dit, c'est un bien public qui est disponible. Pour la deuxième couche, c'est la couche des personnes qui n'ont pas de liquide. Pour un moyen d'authentification cela permet l'ouverture des comptes sans papier. Il peut y avoir des comptes mobiles ou divers. Par exemple, en Inde, certains ont bâti une base de données de client énorme grâce à ce genre d'outils et ils ont pu avoir 2 millions de clients. Cela a été lancé en 2012 et depuis il y a eu 2,5 milliards et cela a beaucoup réduit le coût des opérations. Avant le India Stack, cela a permis que beaucoup de personnes soient incluses dans l'univers numérique. Il y a aussi un niveau, ces fondations - il n'a pas besoin d'être là physiquement. Le deuxième facteur d'identification peut être effectué sans la présence physique de la personne. Le troisième niveau est le niveau sans liquide et sans papier. C'est un système qui a été développé par une entreprise indienne et c'est une entité qui est détenue par 56 banques commerciales. Ils ont créé un bien public qui n'aurait pas été possible autrement. Cela a créé une adresse de paiement virtuel pour chaque client et c'est en marche 24 heures sur 24 et il y a une architecture d'interopérabilité et cela peut être géré sur diverse banque et des fournisseurs des services financiers numériques. Il y a plus de 55 banques qui sont impliquées dans ce système et un milliard d'opérations et 2,6 milliards de roupies. L'UPU a été un grand

bien pour les paiements au détail. Ils ont des petits paiements et dû aux coûts très bas cela a été très population. L'UPU a aussi ouvert un système, mais sous réglementation. Même si les personnes qui ne sont pas des fournisseurs des services peuvent quand même faire partie de ce système UPU. Le dernier niveau est le niveau de pas besoin de présence. Ces données peuvent être obtenues à très petit coût et dans le niveau de consentement la philosophie c'est que l'utilisateur reçoit le pouvoir d'avoir ses propres données et avant les données était en silo, n'est pas apporté dans le compte, mais cette entité se comporte en tant que gestion du consentement pour le transfert des données du client aux entités diverses et l'entité même ne peut pas le voir. Comme je l'ai mentionné, ce système a créé un système d'interopérabilité et une plateforme d'interopérabilité et la réglementation d'avoir un niveau d'agent d'interopérabilité et les parties prenantes collaborent pour avoir une interopérabilité pour le client dans ce cadre. Comme je l'ai mentionné, comme nous sommes régulés par le système, il s'agit là d'une infrastructure de résilience. Finalement, pour les paiements de la poste indienne, les principes sont l'accessibilité et il y a - nous avons multiplié l'infrastructure rurale par 2,5 et avons réduit la distance à une banque de dix kilomètres à cinq kilomètres et avons réduit les défis d'accessibilité. Les produits que nous offrons sont des produits basés sur la technologie. Comme je l'ai mentionné, avec l'aide de l'UPU et d'autres systèmes, la poste indienne a créé une architecture et un réseau bancaire d'interopérabilité par le biais duquel on peut avoir accès à toutes les banques. Vous avez un téléphone mobile connecté et tous les comptes bancaires peuvent être gérés depuis ce dispositif.

Comme je l'ai dit, pendant le temps de la COVID-19, beaucoup des fournisseurs de services n'ont pas pu travailler et le Gouvernement indien a dû envoyer des fonds aux individus. Et les industries et les transactions ont presque triplé et les opérations se sont multipliées par dix. C'est une réflexion sur la résilience et la stabilité de

l'infrastructure qui a été créée que nous pouvions très facilement fournir ce genre de volume sans grand problème. Pour l'avenir, comme je l'ai mentionné, nous allons avoir cette infrastructure en tant que bien public. Le coût peut être un peu élevé pour accroître l'interopérabilité parmi tous les régulateurs et créer des redondances dans les infrastructures des paiements. En dépit du fait que ce programme se débrouille très bien, il y a la banque de l'Inde qui a envoyé des propositions pour inclure des nouvelles parties prenantes. Les produits numériques intelligents pourront être utilisés par la population rurale et en dernier c'est la construction de la capacité en tant que dernier kilomètre. Ces services peuvent être mis à la disposition de toutes les personnes. Je suis prêt à toutes les questions après cela. Merci.

**>>BILEL JAMOUSSE** : Merci, Messieurs Khan et Singh, d'avoir partagé avec nous l'exemple de l'UPU et du service postal au niveau mondial et les exemples concrets de l'Inde et comment le Gouvernement indien a été capable de bâtir 360 millions de comptes d'épargne et d'opération financières sur la base des données partagées avec nous.

Mesdames et Messieurs, nous passons maintenant à la foire aux questions. Je vois que quelques questions ont déjà été reçues. Nous avons déjà reçu des questions. Une question pour Dorothée. Très bonne présentation très détaillée. Est-ce que vous pouvez détailler un peu plus sur quand est-ce que les gens pourront se servir des critères d'évaluation pour le Fonds monétaire international et comment la résilience et la sécurité sont intégrées dans India Stack -- question pour Abhinav Pratap Singh.

**>>ABHINAV PRATAP SINGH** : Merci, Bilel. Comme je l'ai mentionné, le India Stack, chacun des niveaux est régulé au sein du cadre régulateur. Il y a des protocoles de sécurité très élevés. Il y a presque un accès qui est permis pour chacun de ces niveaux. Chacun est contrôlé de façon indépendante. Le ministère des informations gère le niveau sans liquide qui est géré par une autre entreprise indienne. Le niveau

de consentement est géré. Chacun de ces niveaux est géré de façon indépendante par les régulateurs et au sein du cadre cela existe au sein du système entier.

**>>BILEL JAMOSSI** : Dorothee a dû prendre un autre appel. Elle n'est pas disponible pour répondre à la question, mais nous serons heureux de faire le suivi. Nous avons sept minutes qui nous restent pour ce webinaire. Anant, tu as mentionné que tu as un modèle préféré en ayant étudié ces modèles d'interopérabilité, est-ce qu'un est meilleur qu'un autre dans un marché émergent?

**>>ANANT NAUTIYAL** : Tous les modèles sont soutenus par des personnes qui sont très solides. Tout le monde veut que la sienne gagne, donc j'espère que personne ne va me faire de reproches; c'est une question difficile parce que c'est comme si on demandait s'il y a une bonne façon de construire un pont. Pour faire cela, il faut inspecter le pont, est-ce que c'est un grand pont, les conditions, c'est ce genre de question. En dépit de cela, je vais donner une réponse claire en ce qui concerne ma partie à moi. Je regarde toujours quatre choses quand on discute le meilleur modèle d'interopérabilité. Il y a le coût, premièrement. Si vous voulez un système trop cher, cela ne va pas réussir. Il faut aussi regarder la question de l'extension et la flexibilité du système. Il faut être solide et robuste. Cela revient à la question de résilience. S'il y a un problème, il faut pouvoir s'en remettre. Finalement, le problème de la gouvernance, il faut pouvoir être responsable. Si vous répondez à ces questions quatre questions, cela va indiquer la marche à suivre. Dans le marché où nous nous trouvons, vous pouvez choisir tous ces modèles, mais nous pensons que si un seul marché avait été détenu par l'industrie mobile et si vous devez choisir le meilleur service, il y a plusieurs initiatives et il y a eu des initiatives lancées par des grandes entités. Ces initiatives seraient les meilleurs pour nos parties prenantes. Nous ne savons pas si ces initiatives vont réussir mais ce serait notre modèle préféré si tout se passe bien. C'est ma réponse.

**>>BILEL JAMOUSSEI** : Merci. Nous avons fini peut-être présentation. Je vais donner la conclusion. Je vais offrir à tous les intervenants une minute chacun pour des remarques de conclusion. Je commence avec Kevin.

**>>KEVIN BUTLER** : Merci de l'occasion d'avoir parlé aujourd'hui et merci à tous les intervenants. J'ai beaucoup appris sur cette question et j'espère que les autres aussi. Une des choses qu'on peut dire sur l'interopérabilité et la résilience, c'est que ce sont des éléments critiques sur l'écosystème des services financiers numériques. Chaque personne aura sa propre situation différente des autres. C'est un défi à long terme. Nous avons des solutions très réussies qui développent un contexte spécifique pour pouvoir collaborer avec les autres. Mais donc, c'est l'un des grands défis de l'heure actuelle, surtout maintenant avec la COVID-19 et le rôle accru des paiements numériques. Pour que les utilisateurs puissent interagir avec les autres, c'est crucial.

**>>BILEL JAMOUSSEI** : Monsieur Khan.

**>>SALEH KHAN** : Merci, Bilel. J'aimerais souligner le fait qu'il y a des parties prenantes du système, de l'écosystème et nous voulons nous assurer que le gouvernement y travaille et qu'il fournisse un niveau de services fantastique financier pour la population vulnérable qui se trouve dans des circonstances difficiles. Depuis la présentation de la poste indienne, leur système est fantastique. Nous voulons nous assurer que nous soulignons ces exemples et nous demandons aux régulateurs d'être conscient de ce genre d'infrastructure et nous les invitons à visiter notre site Web à la fin de la présentation pour voir ce que fait la poste en ce qui concerne les services financiers. Merci à mes collègues de l'UIT d'avoir organisé ce webinaire.

**>>BILEL JAMOUSSEI** : Merci, Monsieur Khan. Je vais inviter Monsieur Singh à faire des commentaires avant de terminer.

**>>ABHINAV PRATAP SINGH** : Merci, Bilel. Comme je l'ai mentionné et je vais répéter, cela peut être des parties prenantes en ce qui

concerne l'inclusion financière pour un système équitable. Il y a un grand potentiel pour avoir un système de paiement d'interopérabilité auquel beaucoup de parties prenantes peuvent avoir accès. Si on peut avoir un système bien régulé, beaucoup d'entités peuvent collaborer et cela peut faire des miracles comme en Inde. Cela aurait pu prendre 47 ans, mais en fait l'Inde l'a fait en huit à neuf ans. À nouveau, j'aimerais dire comme je l'ai dit dans ma diapositive de l'avenir, il y a une exigence que beaucoup de régulateurs se réunissent et bâtissent et y travaillent pour aller de l'avant. Merci de cette occasion et de m'avoir laissé participer à ce webinaire. Merci.

**>>BILEL JAMOSSI** : J'aimerais remercier tous les intervenants, les participants de ce webinaire et remercier mes collègues, Vijay, Gifty et toute l'équipe qui a rendu et préparé ce webinaire. Nous revenons en septembre pour des épisodes supplémentaires. Nous allons avoir des épisodes préenregistrés en août entre autres sur les combines Ponzi. Je vous remercie de votre participation et bonne journée à tout le monde.

Le webinaire est terminé. Merci beaucoup.