FICHIER NON ÉDITÉ COMPLÉTÉ

Webinaire # 8 — Gestion des délits et des escroqueries de la finance numérique

UIT -- Genève

30 JUIN 2020, 15 h

Services rendus par:
Caption First, Inc.
P.O. Box 3066.
Monument, CO 80132.
1 877 825 5234.
+001 719 481 9835.
www.captionfirst.com

***

***

>>BILEL JAMOUSSI : Bonjour, bon après-midi, bonsoir et bienvenue dans le huitième épisode des aperçus sur les services financiers numériques lors de la série de webinaires COVID-19 organisée par l'UIT. Nous espérons que vous, votre famille et vos amis et collègues êtes tous en bonne santé et en sécurité. Je m'appelle Bilel Jamoussi chef du groupe des groupes 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 comment gérer les crimes et les escroqueries financiers numériques pendant COVID-19. Avant de présenter les panélistes, je fournirai des informations générales sur la logistique du webinaire d'aujourd'hui.

Nous avons beaucoup de participants aujourd'hui enregistrés. Il y en a de plus en plus qui se joignent à nous pendant que je vous parle. Toutes les présentations seront disponibles après le webinaire sur le site Web de l'événement. J'ai le plaisir d'annoncer que nous avons le sous-titrage en français pour le webinaire d'aujourd'hui et je remercie la sténotypiste et l'interprète de rendre ce webinaire plus accessible. Toutes les questions des participants seront prises à la fin de toutes les présentations pendant la période des questions/réponses et les participants peuvent soumettre leur question dans les questions/réponses qui se trouvent au bas de l'écran. Lorsque vous soumettez une question, j'invite les participants à taper d'abord le nom du membre du panel suivi de la question même. Si la question est adressée à tous les membres du panel en général, veuillez bien taper la question directement sans mentionner le nom de l'expert. Le webinaire est enregistré et l'enregistrement sera mis à la disposition du public sur le site Web du webinaire plus tard dans la semaine. Je vais introduire nos experts. Les intervenants vont prendre le micro vont prendre la parole dans l'ordre suivant. Mohammed Imran de INTERPOL, Jami Solli de GALA, Mercy Buku consultante et Niyi Ajao du NIBSS. Dans cet épisode, nous examinons les différents types de délits de la finance numérique, les attaques d'hameçonnage et les escroqueries qui ont connu une augmentation au cours de la COVID-19. En 2020 la pandémie mondiale de COVID-19 a bouleversé les règles du jeu, tenant compte des nouveaux risques et tendances ayant un impact sur le volume et la nature des vecteurs d'attaque.

Selon l'équipe Microsoft de protection d'intelligence, tous les pays du monde ont vu au moins une cyberattaque sur la COVID-19 et parmi les message ciblés nous voyons environ 60 000 impliquant des pièces jointes malveillantes liées eux COVID-19, y compris les attaquants usurpant l'identité d'entités établies comme l'OMS et d'autres organisations liées à la santé pour tirer parti de la crédibilité de ces organisations pour inciter les gens à cliquer sur des liens dans des courriels non

sollicités. Ils criminel ciblent les personnes qui cherchent à acheter des fournitures médicales en ligne envoient des courriels offrant un faux soutien médical et arnaquent les personnes qui peuvent être vulnérables ou de plus en plus isolées à la maison. Ces fraudes tentent de vous attirer avec des offres qui semblent trop belles pour être vraies, comme des investissements à haut rendement et des opportunités de soins de santé ou lancent des appels pour que les gens soutiennent de fausses associations ou ceux qui sont malades. Des rapports du public ont déjà inclus des escroqueries en ligne où des gens ont commandé des masques protecteurs, un désinfectant pour les mains et d'autres produits qui ne sont jamais arrivés et un certain nombre de cas ont été identifiés où de faux kits de test ont été proposés à la vente. Les criminels utilisent également l'image de marque du gouvernement pour tenter de tromper les gens et de faire des fausses offres de soutien financier pour le biais de courriels, d'appel téléphonique et de SMS non sollicités. Cette situation devrait se poursuivre, les criminels cherchant à exploiter les conséquences supplémentaires de la pandémie, par exemple en exploitant les préoccupations financières pour demander des frais initiaux pour des faux frais en offrant des escroqueries d'investissement à haut rendement ou en ciblant les pensions. Les augmentations énormes du nombre de personnes travaillant à distance signifient que beaucoup plus de personnes seront vulnérables à la fraude des services informatiques où les criminels vont essayer de vous convaincre de donner accès à votre ordinateur ou de divulguer vos informations de connexion et vos mots de passe. Les particuliers et les entreprises doivent être pleinement conscients et préparés. Les partenaires des forces de l'ordre du gouvernement et du secteur privé travaillent ensemble pour encourager les membres du public à être plus vigilants contre la fraude, en particulier concernant le partage de leurs informations financières et personnelles, alors que les criminels cherchent à tirer parti de cela. Dans le cadre d'une initiative, il y un programme conjoint de l'UIT de la Banque mondiale

soutenu par la fondation Gates, soit le groupe de travail sur la sécurité l'infrastructure et la confiance dirigée par l'UIT qui a produit un rapport technique mettant en évidence les problèmes de l'investissement numérique sans licence. Nos experts vont nous aider à naviguer dans le paysage des crimes financiers numériques pendant ce webinaire. Maintenant, passons à notre premier intervenant. Je vais les inviter à faire leur présentation et chaque intervenant a 15 minutes environ et notre premier intervenant est Mohammed Imran. Vous avez le micro pendant 15 minutes. Je vous prie.

>>MOHAMMED IMRAN : Merci, Bilel.

Bonjour, bonsoir à tout le monde. Là où que vous puissiez être, j'espère que tout le monde est en bonne santé. Ici à Singapour, je vous dis bonjour. C'est le soir, ici. Je m'appelle Mohammed Imran de l'unité de INTERPOL. Bilel a bien résumé le webinaire d'aujourd'hui. Merci à l'UIT d'avoir organisé cette série de webinaires pour couvrir le résultat de COVID-19, l'impact de COVID-19 au niveau numérique.

Nous pouvons apprendre comment mitiger les risques. Je vais commencer ce webinaire en partageant la perspective de INTERPOL sur certains crimes numériques. Bilel a dit que c'est le cas, les criminels adoptent une nouvelle démarche pour prendre avantage de la situation.

Les régulateurs et les membres du secteur privé vont s'inclure pour se battre contre ce phénomène. Je vais commencer par partager un résumé de la structure mondial de INTERPOL. INTERPOL est compris de deux parties ; notre Secrétariat général avec le siège social à Lyon et des représentants à Singapour et partout dans le monde. Deuxièmement, tout aussi important, nous sommes 194 pays membres et ils sont tous responsables que les agences de respect de la loi sont consultées à ce sujet.

Bien sûr, le crime est très présent au niveau numérique. Cela rend le travail de INTERPOL encore plus important à ce sujet et pour soutenir tous nos pays membres. La prévention du crime, nous avons émis un avertissement en ligne et nous avons publié au début mars un guide

d'avertissement sur les fraudes liées à la COVID-19. Depuis cela, nous avons reçu beaucoup de mises à jour. Et nous n'avons jamais été aussi occupés au niveau quotidien ou hebdomadaire. C'est lié à tous les crimes des pays. Un autre de nos mandats est de soutenir les enquêtes dans nos pays membres. INTERPOL ne conduit pas d'enquête elle-même, mais elle collabore avec les agences d'application de la loi internationale et en gardant une communication constante par notre réseau. Donc, c'est crucial et les fonds concernant les crimes sont déplacés au niveau local et international.

Vous voyez sur la diapositive ici, c'est montré aussi dans les actualités et les nouvelles au niveau mondial. Nous allons regarder les tendances concernant les crimes. Il y a deux éléments ; l'ingénierie sociale où les victimes sont manipulées pour fournir des informations financières et les transferts outre-mer dans le cadre de ces crimes. Le premier crime est la fraude des paiements d'avance en consommant des produits pour la COVID-19 comme les masques et le désinfectant pour les mains. ils font des fausses factures et c'est une version plus technique de ce qu'on appelle BET, le compromis par courriel du business. Ils ajoutent à leur crédibilité en se servant de ce moyen et pour avoir l'air plus légitime. Deux soucis que nous avons à ce sujet, c'est que les montants sont énormes et cela peut s'élever jusqu'à des millions de dollars. Deuxièmement, la fraude est souvent découverte très tard, seulement quand la vérification est effectuée par téléphone. Donc, souvent, comme cela se passe par Internet ou par courriel, on perd la touche humaine et les criminels en tirent parti. Jusqu'à ce que ce soit découvert, les criminels ne peuvent pas être découverts et l'argent est perdu.

Donc, c'est très difficile à récupérer les fonds. Donc, à ce sujet, nous vous invitons à être très vigilants, surtout lorsqu'il s'agit des gros montants. Mettez en place des mesures pour que ce ne soit pas soumis à des erreurs humaines. Le deuxième crime est la fraude de personne et c'est l'hameçonnage lorsque le criminel fait semblant qu'il est un

organisme pour voler des fonds auprès des victimes. Comme Bilel l'a dit, ils ont même fait des schémas de COVID-19 pour le combattre; il faut essayer de mettre au courant le public et d'atteindre tous les niveaux de la société et ne pas cliquer sur ces liens qui sont un peu louches.

Les criminels prennent parti de la grande demande de vaccins surtout lorsque la demande est très élevée, il y a un marché pour les produits frauduleux. Beaucoup de pays se sont joints à une enquête à ce sujet; 48 000 produits médicaux faux ont été saisis. Il y a eu 2500 liens de site Web qui ont été fermés et beaucoup de criminels arrêtés.

Finalement, la fraude des dons. Les criminels essaient de cibler les personnes généreuses parmi nous et c'est très créatif. Ils font semblant d'être des amis légitimes et il y a une histoire très triste en leur disant qu'il faut de l'argent pour des pauvres malades victimes de la COVID-19. C'est très impressionnant qu'ils soient tellement créatifs, mais c'est une grande fraude. Comme nous le savons bien, lorsque la COVID-19 sera terminée, nous serons en récession économique et là il y aura d'autres crimes qui vont se montrer. Nous ne voulons pas faire de prédictions, mais nous devons savoir ce qui nous attend pour pouvoir mettre en place des ressources et des mesures. Premièrement, ce sont les crimes qui sont permis, des crimes liés à l'Internet. Il y en a déjà eu beaucoup, mais il va y en avoir plus à l'avenir. Il y aura des crimes Internet, de cybersécurité, des domaines malveillants et des attaques sur des institutions de santé, des hôpitaux. INTERPOL a fait une campagne de prise de conscience mondiale pour faire la promotion d'une bonne hygiène. Il faut faire des recherches sur qui fait ce site parce que les criminels créent des faux sites Web rapidement. Un autre crime qui va émerger dans les pays sera la mule d'argent. La mule d'argent va beaucoup se développer en raison de la COVID-19. Beaucoup de personnes seront recrutées à titre de mules d'argent. Et ce pour satisfaire aux besoins d'argent. D'autres crimes

susceptibles de se montre seront des crimes liés aux prêts qui créent des crimes au niveau des prêts bancaires et la fraude sera susceptible de faire partie de cet environnement. Maintenant, il y a un besoin d'agir rapidement pour éviter l'effet de ces crimes.

Nous avons un outil qui s'appelle les avis INTERPOL. Nous nous concentrons sur les avis rouges, bleu et violet. Ce dernier avis en violet avise les pays de partager leur mode d'opération. J'aimerais prendre cette occasion d'inviter tous les pays à se joindre à cette initiative. C'est là où le secteur privé et les régulateurs peuvent se joindre. Les services d'application de la loi ne seront pas les premières victimes, mais c'est très urgent pour que le secteur privé et les autres émettent des avertissements très rapidement pour donner le temps aux agences de régulation et d'application de la loi de prendre action.

Dès qu'il y a eu une fraude, il faut le signaler dans les 48 heures. Il y a une application de la loi d'une façon efficace c'est d'établir des unités antifraude dans votre pays pour avoir un point de contact direct. Cela accroît la possibilité d'exécuter des mesures prévisionnelles pour couper les crimes financiers. Nous encourageons les pays pour implanter des approches multiniveau pour combattre ces crimes. Il y a plusieurs formes ; il y a d'abord une collaboration accrue avec les partenaires. Il y a d'autres canaux à part INTERPOL avec beaucoup de réseaux financiers et d'intelligence. Deuxièmement, il y a les secteurs privés et publics qui présentent beaucoup d'information sur le secteur privé et c'est crucial de prendre contact avec ce genre d'organismes. Le plus vite on se met en marche, le mieux. Une plateforme doit être établie et cela peut être initié par une conversation avec une banque ou plusieurs banques dans le pays. Finalement, la sensibilisation à ce problème surtout pour les personnes les plus vulnérables est importante. Il faut à nouveau une bonne collaboration entre le secteur privé et les agences d'application de la loi pour maximiser les effets de cette action.

La fraude de la COVID-19 nous fait face et il faut être conscients qu'il y a beaucoup de possibilités et d'occasion de collaborer et de nous battre. La collaboration entre le secteur privé et les agences d'application de la loi doivent être renforcées et une solution est là. C'est la fin de mon discours. N'hésitez pas à me poser des questions. Bilel, je te rends le micro.

>>BILEL JAMOUSSI : Merci, Mohammed de INTERPOL, pour ton excellente présentation au niveau d'hameçonnage et des escroqueries et du crime au niveau mondial.

Nous allons revenir vers toi avec des avez, il y a déjà des questions ajoutées dans la boîte des questions/réponses. Je te remercie et je passe au prochain intervenant. Merci beaucoup. La consultante juridique, vous avez un quart d'heure.

>>MERCY BUKU : Merci beaucoup.

>>BILEL JAMOUSSI : Pendant que Madame Buku se prépare... merci, vous avez la parole.

>>MERCY BUKU : Merci. J'espère que tout le monde peut me voir et peut voir ma présentation.

>>BILEL JAMOUSSI : Oui, oui.

>>MERCY BUKU : Merci. Je vais faire une révision des crimes financiers numériques que nous avons vus du point de vue africain. Merci de nous donner une très bonne perspective au niveau international, Imran. Je vais vous donner un petit historique du genre de fraude que nous avons vu et vous parler de pourquoi nous sommes vulnérables en Afrique pour le genre de fraude que nous voyons. Ce ne sont pas des fraudes qui sont nouvelles, mais nous voyons une augmentation pendant l'ère de la COVID-19. Imran a parlé d'Internet et des options disponibles sur Internet et le genre de crime sur Internet. Mais pour nous ce qui est réel et surtout pour les utilisateurs des services financiers numériques sur téléphone, tout le monde en a un, il y a l'anonymat du service et cela les rend vulnérables à la fraude. La prolifération de tous les produits disponible actuellement sur

certaines plateformes mobiles financières les rend vulnérables aux crimes. Bien sûr, les services et les paiements numériques, les transferts d'argent, les services de banque mobile. En partenariat avec les opérateurs financiers mobiles. Ce que je veux dire ici, c'est que ces produits fournissent des opportunités de fraude et d'activités criminelles et aussi la vulnérabilité est accrue pendant l'ère de la COVID-19. Et aussi du fait que le gouvernement encourage les paiements sans liquide. Nous avons parlé de la fraude ; elle nous est familière. Au Kenya, ce qui a été lancé en 2007, nous avons eu beaucoup de fraudes en Afrique de l'Est. Mais comme la pandémie de la COVID-19 s'est répandue très vite dans tous les côtés de l'Afrique. Maintenant, cela se trouve aussi en Asie. Ce sont des fraudes communes catégorisées sous trois niveaux. Nous avons les fraudes d'identité et les personnes qui envoient de l'argent à quelqu'un qui refuse de le rendre ; les fraudes d'usurpation d'identité. Il y a quelqu'un, il y a des gens qui se servent de fraude sur les comptes bancaires avec de l'argent faux. Aussi, dans des candidatures pour demander du travail qui sont contrefaites. Les dépôts d'argent contrefaits, des comptes bancaires frauduleux. Des clients vont payer pour des services et lorsque le marchand demande à voir le message, on leur montre un message faux contrefait pour une opération précédente. Tout cela se passe et cela a un impact. Si vous considérez les fraudes communes qui ont impacté les fournisseurs la fraude interne, la fraude mobile et la fraude de crédit numérique et l'utilisation illégale des plateformes mobiles aux fins d'activité criminelle comme le blanchiment d'argent et le financement du terrorisme.

Il y a aussi des fraudes au niveau des prêts. Ils prennent des prêts et ne paient pas. Et d'autres plateformes d'activités criminelles. En gros, c'est le statu quo avant la COVID-19. Quelles ont été les vulnérabilités pendant l'ère de la COVID-19 ?

Nous avons vu une augmentation des fraudes, d'anciens modes de

fraude, parce qu'il y a de plus en plus de paiements sans liquide et numériques. Par exemple, si vous ne pouvez pas aller rendre visite à votre pays d'origine ou à votre supermarché, vous commandez en ligne et vous payez en ligne avec de l'argent mobile. Ou avec un paiement numérique. Les gouvernements dans la plupart des pays ont fait la promotion active pour les paiements sans contact et se sont mis d'accord avec les fournisseurs pour réduire les frais liés à ce sujet. Ils ont découragé l'utilisation du liquide. Les différents magasins préfèrent être payés non en liquide. Il y a des paiements non liquides, mais (la connexion a été interrompue) — beaucoup de nouveaux produits ont été découverts et les frais ont été baissés de façon importante. Par exemple, au Kenya, jusqu'à dix dollars de transfert pour les banques mobiles ont été réduits, jusqu'à zéro. Nous avons même un soutien, un secours au niveau fiscal. Auparavant, vous pouviez avoir 1 000 $ avant de faire l'objet d'impôt, mais maintenant vous pouvez transférer encore plus, jusqu'à 3 000 $ avant de faire l'objet d'impôt. La fraude et les fournisseurs, les criminels ont leur propre entreprise, leurs propres affaires et ils ont beaucoup d'escroquerie sur le marché.
L'augmentation des volumes d'opération a deux systèmes qui peuvent mener à des temps où le système ne fonctionne pas. Il y a aussi des problèmes de risque de conformité. Le personnel travaille depuis chez eux et il ne sera pas possible de surveiller les services mobiles des banques. Donc, il y aura des défis de conformité et de surveillance des agences et des branches des banques. Il n'y aura pas d'audit et bien sûr en dernier il y a le risque économique qui est dû à des niveaux de pauvreté accrus dus à la clôture des commerces qui découle du confinement et d'autres mesures COVID-19 qui ont un impact surtout sur les personnes à revenu faible.

Nous avons tout cela qui se passe; lorsque quelqu'un n'a plus de ressources, ils vont essayer d'obtenir des revenus sur la base de moyens criminels.

Voici les fraudes les plus communes ; il y a trois catégories qui ont un impact sur le consommateur : la candidature d'emploi, la fondation Gates ont fait de la publicité pour la fourniture de certains services et les gens devaient payer un montant pour le matériel et c'était une escroquerie. La fondation Gates a émis un avertissement pour dire que c'était une escroquerie. Mais si quelqu'un vous envoie un message pour envoyer de l'argent là. Si vous devez envoyer de l'argent à quelqu'un, assurez-vous que ce n'est pas une escroquerie. Pour l'impact sur les agents, ce n'est pas tellement parce que les personnes ne rendent pas visite à des représentants, donc, cela va peut-être être en réduction. À part les escroqueries promotionnelles et d'usurpation d'identité. Ces dernières pourront s'accroître. Le troisième, c'est l'impact sur les fournisseurs. On peut s'attendre à des fraudes internes et numériques.

Pour conclure, je veux considérer les mesures d'atténuation. Ce n'est pas du point de vue du fournisseur. Les fournisseurs ont déjà mis cela en place. Il faut mettre en place des mesures de diligence accrues en raison de l'enregistrement en ligne et pour les volumes d'opération accrus. Ils ne prennent pas à bord des personnes qui ont des identités troubles ou fausses. Il y a aussi deuxièmement les campagnes de sensibilisation en ligne sur les médias sociaux et tous les réseaux sociaux. Qu'est-ce qu'il faut faire pour se protéger ? Les canaux d'aide aux plaintes ou aux réclamations ; les fournisseurs doivent maximiser ce côté-là. Nous devrons aussi faire un dépistage et une surveillance des opérations, surtout dû aux limites d'opérations qui ont été révisées pour la COVID-19. Les fournisseurs doivent accroître la capacité de surveillance à ces niveaux en raison du volume en augmentation.

Cinq. La gestion des représentants. Il faut qu'il y ait une évaluation des risques pour les nouveaux produits pour identifier des nouveaux risques et mettre en place des contrôles d'atténuation. Les contrôles

techniques axés sur les utilisateurs et les contrôles de mots de passe et les nouveaux portefeuilles mobiles. Les fournisseurs doivent mettre cela en place. Initialement, il faut collaborer avec les agences d'application de la loi pour pouvoir arrêter et identifier les suspects. Ensuite, la coopération entre l'industrie et les parties prenantes et il doit y avoir un partage d'information mutuel et des mesures de protection des consommateurs. Il faut aussi des mesures de régulation et de surveillance pour la gestion des risques et la surveillance de la conformité. Une petite diapositive pour terminer ; c'est une nouvelle mesure mise en place chez Safaricom. C'est une prévention pour les échanges ; quelqu'un essaie de vous attendre en utilisant votre identifiant et vous allez recevoir un avis pour approuver oui ou non et c'est une bonne mesure préventive et vous allez appuyer sur « non » bien entendu. Je vous ai donné seulement un aperçu et je crois que maintenant nous allons recevoir du prochain intervenant une perspective nationale.

>>BILEL JAMOUSSI : Merci beaucoup de votre perspective sur la situation en Afrique, surtout pendant et après COVID-19. Et comment tous les pays se servent des services numériques ? Cela a ouvert la porte à beaucoup d'escroqueries et de crime et votre proposition pour commis remédier. Je vous remercie d'avoir partagé votre perspective à ce sujet.

Je vais passer à notre prochain intervenant, Madame Jami Solli. C'est une avocate de protection. Vous avez le micro pour 15 minutes.

>>JAMI SOLLI : Bonjour et merci de vos présentations si intéressantes. À l'heure actuelle, je veux remercier l'UIT d'avoir mis en place ce sujet et comme le titre de ma diapositive le montre — est-ce que vous voyez ma diapositive ?

>>BILEL JAMOUSSI : Je vois votre écran et le titre.

>>JAMI SOLLI : Désolée.

>>BILEL JAMOUSSI : C'est bon maintenant.

>>JAMI SOLLI : Désolée, je veux mettre ma présentation. Comme le titre le suggère, je vais parler des programmes d'investissement numérique sans licence. Est-ce que c'est un crime financier d'orphelin ? Cela n'a pas reçu assez d'attention de la part des autorités nationales ou des parties prenantes, alors je remercie l'UIT d'avoir pris en charge ce sujet. C'est un crime qui a toujours été présent et nous nous attendons à ce que cela continue et augmente dès la fin de la COVID-19.

Je crois que c'est déjà actuellement dans le monde d'après les statistiques de 2019. Depuis les années 2019, il y a une augmentation de 300 % ; 3 milliards de dollars ont été volés en raison de ces programmes frauduleux. Il y a aussi l'état des crimes encryptés qui a été établi. En ce qui concerne les investissements en ligne, alors 4,3 milliards de dollars ont été volés l'année dernière et nous n'avons aucune raison de croire que cela ne va pas se poursuivre. En particulier, quels sont ces crimes, comment ils opèrent et quelles sont les conséquences au niveau du consommateur et au niveau macro ? En ce qui concerne les conséquences pour les consommateurs, je vais en parler plus tard. J'ai interviewé une centaine de victimes de crimes et j'aimerais parler de résultats personnels et au niveau de leur famille pour nous permettre de comprendre l'urgence et le besoin que nous avons de faire face à ce crime. J'aurai des exemples en particulier qui émanent de l'infrastructure de la FIGI en Inde, Nigeria, Kenya et au Bangladesh il y a eu une recherche en 2016. Ces exemples seront un peu anciens, mais nous n'avons aucune raison de croire que le statu quo a changé. Les crimes sont toujours prévalant et il n'y a pas eu des nouvelles mesures pour faire face à ces crimes. Qu'est-ce que cela veut dire les combines de crimes sans licence ?

Nous discutons la fraude financière qui se passe au niveau numérique et qui offre un grand retour sur l'investissement. Qui offre des grands rendements. Le rendement émane des investisseurs futurs qui investissent dans la combine, mais il n'y a pas d'actifs productifs.

Donc, en général, il y a des combines ; ils se servent des nouveaux fonds pour les investisseurs en place ou ils prennent l'argent et ils s'en vont. Donc, il y a deux mécanismes ; le premier où ils paient les investisseurs en place. Nous appelons cela l'équipe de promotion parce qu'ils vont communiquer à leurs amis et leurs collègues en disant je viens de gagner tous ces sous et ils vont convaincre les autres d'investir dans leur combine ou bien les gens qui le font rapidement et qui s'en vont. Les découvertes clés sur la recherche FIGI, il n'y a pas vraiment un seul meneur de jeu au niveau gouvernemental pour surveiller, faire la prévention ou faire face aux réclamations et aux crimes. Il y a peut-être des acteurs multiples ; au Nigeria il y avait cinq ou six agences gouvernementales y compris la police qui ont pris la responsabilité de faire face à ces combines.

Il y a très peu de poursuites à ce niveau. Nous n'avons eu aucune occasion où les consommateurs ou les victimes ont été compensés pour les fonds perdus pendant notre recherche. La prévention et la sensibilisation des consommateurs sont très limitées et pas constante et quand c'est fait il n'y a pas de mesure de l'impact de ces efforts d'informer les consommateurs. Il n'y a pas de statistique ni de recherche sur l'impact de ces crimes sur l'inclusion financière ou l'exclusion financière. Cela a été un autre point focus de ma recherche ; ce qui se passe sur le Web sombre, le Dark Web. Conséquences des crimes, y compris le blanchiment d'argent. Les victimes, comme je l'ai dit, font l'expérience de stress mental et de souffrance lorsqu'ils perdent de l'argent dans ces combines. Vous verrez des crises cardiaques, de la haute tension, du diabète, souvent des divorces parce que la femme ou le mari qui a pris toutes les économies et les a mises dans une combine frauduleuse ; imaginez les conversations autour de la table du dîner quand quelqu'un annonce que les économies de la famille sont perdues. J'ai suggéré que l'impact est aussi entre les générations, les enfants ne peuvent plus aller à l'école parce qu'on ne peut plus payer leurs

frais de scolarité et au pire il y a les suicides. En ce qui concerne l'inclusion financière ou l'exclusion financière, les victimes ont souvent emprunté et ont contracté des prêts auprès de banques commerciales ou d'institution de microfinancement et ils ont perdu l'argent et ne peuvent pas repayer. On a vu quelque chose grâce aux données fournies qui montrent qu'une combine qui était en existence pendant six mois au Nigeria a pu prendre 70 millions de dollars américains en six mois d'activité frauduleuse. Cela, c'était une seule combine. C'est plus que le budget de scolarité du gouvernement du Nigeria. Donc, cela c'est très représentatif de ce qui se passe à l'heure actuelle. Pourquoi ces crimes s'épanouissent ? Mercy en a parlé et elle a parlé de la vulnérabilité des personnes, surtout à l'ère de la COVID-19. Mais c'est dû aux réseaux sociaux et dû à la publicité gratuite, vous pouvez aller sur Facebook, YouTube, Instagram et Twitter et tapez occasion d'investissement et vous allez trouver énormément d'exemples de combines frauduleuses potentielles. Donc, nous avons des standards de communauté sur Facebook, par exemple, qui disent que ce genre d'affiches vont être descendues et ne devrait pas être sur les réseaux sociaux, mais nous ne voyons pas vraiment d'application de ces standards de communauté.

Au vu de l'utilisation des réseaux sociaux très élevée parmi les jeunes, nous verrons les jeunes plus ciblés par ces crimes et cela a été prouvé par des recherches faites en Afrique de l'Est en ce qui concerne les emprunteurs numériques. Et la plupart sont jeunes, des hommes et on peut voir d'après les données que la plupart vont obtenir des prêts et les repaient et l'impact c'est qu'ils vont obtenir une plus grande offre de la part du prêteur. Donc, ils sont très vulnérables. Un pourcentage de jeune se sert de leur prêt pour faire des jeux au casino et cela va peut-être des paris pour jouer et cela va les rendre vulnérables à des combines frauduleuses. Du point de vue des réglementations, il y a une petite réaction, mais pas assez et trop tard.

Le message émanant du gouvernement n'est pas vraiment approprié pour arrêter ces crimes. Ce qui se passe c'est qu'une banque centrale, le SEC par exemple au Nigeria va émettre un message sur leur site public. Les membres du public, la troisième ligne avec l'avis en jargon juridique, vous avez perdu votre public ; cela y est. D'abord, le grand public ne va pas regarder tous ces avis émis par les banques centrales.

La façon dont c'est formulé doit changer et cela doit être formulé dans un langage accessible au grand public.

Cela doit être affiché dans les réseaux sociaux. S'il n'y a pas assez de personnel à la banque centrale ou dans les agences d'application de la loi, nous suggérons que ces réseaux sociaux embauchent des jeunes au chômage qui vont émettre des avis dans leur propre langage pour avertir leurs pairs de se méfier. Ils se servent aussi des influenceurs en ligne pour émettre leur fraude. Pour le rapport complet que j'ai mis en ligne, nous avons 13 recommandations qui se concentrent sur la réglementation et sur les parties prenantes qui sont intéressées à collaborer. L'UIT a déjà fait un magnifique travail en aidant la discussion à se propager et en unissant les acteurs principaux pour considérer la marche à suivre face à la COVID-19 et après la COVID-19.

Il faut se rappeler qu'il y a 3,4 milliards de dollars perdus dans ce genre de crime. Parmi les 13 recommandations au niveau national, il doit y avoir une entité gouvernementale responsable et leader du combat. La réglementation financière doit aussi considérer le blanchiment d'argent et collaborer avec d'autres institutions pour faire enquête sur ces crimes. Il doit y avoir plus de surveillance sur Internet et les médias sociaux. Il devrait y avoir un établissement de politiques de compensation. Si vous voyez qu'il y a une transaction soupçonneuse, cette agence pourrait peut-être recevoir une motivation pour rapporter ce crime au niveau officiel. Il devrait y avoir au niveau national une collaboration pour établir une combine de compensation des victimes. Il faut aussi rétablir des pénalités pour les individus et les entreprises qui facilitent consciemment ces crimes et avoir des

dommages punitifs à leur sujet. Ils ont des politiques en place pour dire qu'ils ne soutiennent pas ces crimes, mais ils ne les combattent absolument pas. Et les régulateurs devraient aussi se servir des nouvelles technologies qui peuvent être utilisées sur les réseaux sociaux. Ils devraient faire aussi face au Dark Web. Il faut aussi plus de collaboration au niveau international. Il semblerait que cela n'a pas été un problème pris en considération par les parties prenantes internationales. Il doit y avoir un forum au niveau international qui soutient le réseau et cette entité va réunir le secteur des télécommunications et financier pour avoir une collaboration entre les deux. Mercy a mentionné qu'il y avait une augmentation de ce genre d'activités, il faut une plateforme pour rapporter ces crimes en temps réel, parce que souvent nous n'avons que 48 heures pour arrêter ce crime. Cette même entité doit aussi protéger l'intérêt du consommateur qui est très impacté par ce genre de crime. Il faut beaucoup de travail à ce sujet en collaboration avec les sociétés de protection civile. C'était ma dernière recommandation. Merci à tout le monde. Je me réjouis de la discussion pendant la foire aux questions.

>>BILEL JAMOUSSI : Magnifique. L'avocate de protection des consommateurs, merci beaucoup de ta présentation sur ces crimes et ces combines et l'impact sur les familles et les gens et comment cela a augmenté par la COVID-19.

Le montant de 3,4 milliards de dollars perdus est incroyable. Merci d'avoir partagé la mise à jour sur les groupes de protection de FIGI à ce sujet et tes recommandations pour se battre contre les combines frauduleuses. Nous reviendrons vers toi avec plus de questions dans un minimum. Je te remercie pour ligue.

Je souhaite la bienvenue à Niyi Ajao pour une mise à jour du système bancaire du Nigeria. Je te passe le micro.

>>NIYI AJAO : Bonjour, bonsoir, tout le monde. Merci beaucoup. Je suis très heureux de faire partie de ce webinaire. Je remercie l'UIT de m'avoir invité à avoir cette conversation. Je vais me concentrer

sur l'expérience au Nigeria.

Je vais parler de l'escroquerie financière numérique pendant la pandémie comme nous la voyons au Nigeria. Je m'appelle Niyi Ajao et je travaille dans le système d'application des banques du Nigeria. L'impact économique de la COVID-19 est mondial. Comme je l'ai dit, nous voyons des événements avant la COVID-19 et après, dans tous les pays. Cela résume l'impact que nous avons vu et sur les diapositives, il y a l'impact de la COVID-19 sur les commerces. Dans cette diapositive, c'est comparé avec l'expérience au niveau mondial. En 2008, la crise financière mondiale de 2008 et nous avons la même chose en 2008, donc c'est un immense impact. Aujourd'hui, nous considérons l'impact sur les consommateurs.

Tous les secteurs sont affectés. Si nous regardons les consommateurs en particulier au Nigeria — je me concentre sur le Nigeria — nous avons eu au début mars le début de la COVID-19 et nous avons vu beaucoup de clients bancaires se fier à tous ces canaux quoique d'habitude ils ne se servaient pas des canaux numériques pour les services bancaires. Ils se servaient maintenant de leur carte et de leur téléphone pour faire les transferts. Donc, c'est le premier résultat sur les clients. Ils ont commencé à se servir des machines de distribution de billets automatiques et il y a eu plus de concentration sur les paiements électroniques et les paiements par Internet pour payer leurs factures.

Donc, la même chose s'est passée pour le commerce en ligne. Beaucoup plus de paiements en ligne. Comme nous voyons dans le reste du monde, il y a beaucoup de commandes en ligne. C'est devenu très prévalent et les compagnies de logistique sont très occupées. Nous avons vu des agences DFS, l'impact de la COVID-19 sur le liquide est très élevé. Au Nigeria, il y a beaucoup d'endroits où il y a un grand panneau qui dit « liquide non accepté » parce que les gens peuvent être infectés en manipulant des billets de banque. Au Nigeria, ils ont essayé — le Nigeria a essayé de lancer une campagne de paiements non liquides et donc il y a eu finalement un impact sérieux sur la fraude électronique

liée à la COVID-19. Comme on a dit avant, tout reste le même, l'hameçonnage et tout cela reste identique et il n'y a pas eu de changement. Les escroqueries liées au coronavirus en ligne se sont étendues au Nigeria pendant le confinement. Les personnes sous confinement sont des bonnes victimes potentielles. AFP donne un très bon résumé de l'impact de la COVID-19, en particulier au Nigeria. Comme vous le voyez dans cette diapositive, vous avez plus tôt ce mois l'organisme de police criminel international, INTERPOL a trouvé 1,6 million d'escroqueries liées aux masques y compris l'Allemagne, les Pays-Bas et l'Irlande et 500 000 € ont été transférés pour les articles médicaux et émanant du Nigeria. Beaucoup d'escroqueries liées aux masques et ce sont des exemples clairs de problèmes que nous voyons. Vous voyez ici des affiches du gouvernement factices. WhatsApp est devenu très actif, les SMS pour essayer d'atteindre le monde. Pendant le confinement, les criminels ont pris avantage de cela. Vous voyez des escroqueries qui font semblant d'être des agences gouvernementales qui font des promesses. Celui-là en particulier, vous recevez un ventilateur gratuit si vous envoyez tant d'argent et il y a eu beaucoup de personnes qui ont cru que c'était quelque chose de vrai.

Le gouvernement a promis de s'en occuper et de faire face à cette menace. Il y a un autre document gouvernemental factice qui promet, qui dit qu'il faut envoyer de l'argent. Nous allons vous envoyer un crédit dans votre compte bancaire. Et donc, cette escroquerie criminelle, vous voyez que dans ce compte l'argent a été envoyé. Et dans le quatrième exemple qui fait semblant émaner du gouvernement fédéral du Nigeria, on dit de remplir ce formulaire pour pouvoir obtenir de l'argent. Dès qu'on clique, ils obtiennent de l'information pour l'escroquerie. En avril et en mai de cette année, il y a eu des réclamations accrues. Il y a eu des rapports de la police, d'autres organismes gouvernementaux qui ont reçu énormément de réclamations de la part des clients qui ont fait l'objet d'escroqueries et ils recherchaient comment récupérer leur argent. Il y a eu beaucoup de

réclamations, un très haut niveau. Quelque chose d'autre d'intéressant, ce sont des documents philanthropiques faux. La photo, c'est la photo de l'homme le plus riche d'Afrique qui a eu sa photo sur beaucoup de documents contrefaits. Il fait une promesse au peuple du Nigeria en disant que cela va contribuer à telle ou telle bonne action. Et c'est envoyé par SMS.

Et donc, dès que vous envoyez l'argent, ce sont en fait des criminels qui vident le compte bancaire. Donc, les criminels font semblant que ce sont des institutions financières en envoyant des courriels contrefaits et en demandant des informations bancaires sensibles pour des supposés bénéfices en liquide. Par exemple, cette photo de courriel viral fait semblant de représentant une banque en promettant de l'argent une fois que les victimes valident les détails en se servant du lien. Nous avons vu des kits de test qui peuvent donner des résultats rapides ; ne vous en servez pas, c'est un avertissement. Donc, voilà, ne vous en servez pas et c'est émis et c'est une clause de non-responsabilité émise par le NCDC. Toutes ces affiches que vous voyez ici, elles sensibilisent le grand public. Il faut avoir une sensibilisation au niveau de tous ces crimes et de ces fraudes. Les personnes qui voient ces messages d'escroquerie nous le disent et nous les inférons de ne pas les utiliser. Il y a aussi des escroqueries liées au coronavirus que la FTC a averti le monde de faire très attention à ce genre d'escroquerie. Il y a eu aussi des escroqueries au niveau de Medicare émis par la FTC. L'industrie médicale a été très touchée. Le secteur médical avant la COVID-19 était isolé de ces escroqueries, mais depuis l'ère de la COVID-19, l'équipe médicale travaillait encore, donc cela a été très touché par les escroqueries liées à la COVID-19. dès que les banques ont vu que cela se passait, les banques du Nigeria ont émis un avertissement adéquat pour avertir leur clientèle.

Cela par des messages, des SMS, des courriels émis par la Banque mondiale au sujet des imposteurs, des criminels et cela a limité les dommages causés. Plusieurs banques ont fait cela au Nigeria en envoyant

des avertissements à la clientèle pour dire qu'un autre message pour avertir la clientèle de fraudes en faisant semblant qu'ils sont des officiels liés à la COVID-19 et cela a limité les dommages. Beaucoup de clients ont été victimes de ces escroqueries. Il y a trois catégories de comptes client ; il y a trois catégories, les natifs numériques qui sont nés pendant l'ère numérique, deuxièmement il y a ceux assis sur le portail ou qui sont assis sur la clôture et qui ne savent pas où aller et troisièmement il y a les personnes âgées qui sont un peu comme les natifs ou ceux assis sur la barrière. Il y a eu des personnes qui essayaient de prendre avantage. (Coupure de connexion Internet de l'interprète.)

Le plus de sensibilisation des fournisseurs de produits, le moins ces escrocs pourront profiter de la situation.

La prochaine diapositive, c'est la recherche conduite dans 11 pays et les risques de fraude sont en augmentation dramatique au fur et à mesure que les mesures d'isolation de la COVID-19 montent. Comme je l'ai dit, je crois que dans le futur, les CBDC qui vont et les fournitures de produit et toutes les entités doivent sensibiliser de plus en plus le public au sujet de ces fraudes et de ces escroqueries. Merci beaucoup.

>>BILEL JAMOUSSI : Merci beaucoup, Niyi, pour la présentation et surtout sur le CBDC, les convertisseurs COVID-19. Merci beaucoup d'avoir partagé l'expérience au Nigeria, la façon dont le système du Nigeria travaille pour atténuer ces escroqueries et ces fraudes au fur et à mesure qu'elles se déclarent. Et aussi sur les mesures prises pour faire face à toutes les occasions de crimes sur les médias sociaux. Maintenant, nous avons fini les présentations et nous allons passer à la foire aux questions. Pendant que vous tapez vos questions, j'ai une question à adresser à nos experts pour avoir un petit dialogue. À votre avis, que devraient faire les régulateurs et le secteur privé pour lutter contre l'augmentation des délits liés à la finance

numérique liés à la COVID-19 ? Est-ce que mes collègues voudraient bien répondre ? Mohammed, tu étais le premier intervenant, quelle est ton opinion à ce sujet ?

>>MOHAMMED IMRAN : Merci, Bilel. J'ai partagé un peu de cela dans ma présentation à ce sujet. Mais du point de vue de l'application de la loi, j'aimerais voir plus de collaboration entre l'application de la loi, les régulateurs et le secteur privé. Cela peut avoir deux bénéfices : une plus grande chance d'exécuter les applications légales. Et donc, souvent on a que 48 heures pour arrêter un crime et ce n'est pas toujours possible au niveau mondial. Il faut, il y a un niveau de 10 % de recouvert des fonds. C'est toujours une affaire très lucrative pour les escrocs et aussi pour avoir un partage d'information plus efficace entre toutes les parties prenantes. Il faut en faire plus à ce sujet. Deuxièmement, il faut avoir une éducation du grand public. Il faut pouvoir faire face à ce groupe de personnes de façon plus efficace et toutes les parties prenantes peuvent donner leur avis à ce sujet et cela va pouvoir bien contribuer à faire face aux crimes en ligne et numériques pendant cette période.

>>BILEL JAMOUSSI : Merci. Mercy, voulez-vous répondre?

>>MERCY BUKU : Merci beaucoup, Mohammed et Niyi pour nous avoir donné des exemples réels de ce qui se passe. C'est intéressant de voir ce qui se passe au Nigeria. En particulier, pour les régulateurs. Je vais commencer par les fournisseurs, plutôt. Les fournisseurs doivent pouvoir éduquer les consommateurs et la clientèle et les régulateurs doivent implanter des mesures de protection des consommateurs. Beaucoup de pays n'ont pas de loi de protection du consommateur, pas seulement pour les affaires en ligne, mais en général. Cela doit être mis en place et en application. Pour les fournisseurs, Telco aide beaucoup à l'application de la loi au Kenya dû aux données qu'ils ont et un système très raffiné en ce qui concerne les opérations financières. Il doit y avoir plus de collaboration entre les

fournisseurs et les agences d'application de la loi en ce qui concerne les données. Il y a une certaine information pour pouvoir faire la surveillance de ces applications de la loi. Et donc, on ne peut pas axer, souligner l'importance des réseaux sociaux, il faut nous en servir comme des sources très valables des données sur les tendances de fraude et ils peuvent aussi informer les fournisseurs sur les mesures d'atténuation qu'ils peuvent mettre en place.

>>BILEL JAMOUSSI : Merci. Jami?

>>JAMI SOLLI : Je suis d'accord avec les présentateurs, surtout sur la collaboration comme dit Mohammed, la collaboration avec le grand public parce que beaucoup de personnes ont très peur de rapporter cela à la police parce qu'ils ont peur que la police fasse des représailles. Beaucoup de collaboration entre les associations des consommateurs pour avoir une relation très étroite avec INTERPOL et d'autres acteurs de régulation. Nous avons une conversation hors ligne sur comment impliquer les mouvements des consommateurs parce que beaucoup font l'expérience de beaucoup de réclamations pas seulement au niveau du secteur financier, mais au niveau de la fraude. Il faut avoir beaucoup d'information à ce sujet. En ce qui concerne les mécanismes de prévention, il faut vraiment bien regarder, surveiller le réseau social. Beaucoup de pays ont beaucoup de chômage parmi les jeunes et ils sont souvent en ligne. C'est un grand risque pour les pays, mais c'est aussi une occasion pour les pays de se servir de cette jeunesse pour surveiller les réseaux sociaux. Il faut avoir un peu de pensée créative pour mieux disséminer les messages et se servir des jeunes. On leur donne des emplois. Il y a un rôle proactif pour se battre contre ces combines frauduleuses.

>>BILEL JAMOUSSI : Merci beaucoup, Jami. Niyi ?

>>NIYI AJAO : Il faut avoir une sensibilisation du grand public et aussi du secteur privé et des fournisseurs de services. Il faut avoir aussi une collaboration. Il y a un forum au Nigeria qui comprend les fournisseurs de services et la banque et ils se rencontrent de façon

mensuelle en discutant des événements et en se mettant en accord sur des contre-mesures. Il faut poursuivre cela. Je veux aussi ajouter sur la surveillance. Nous devons en faire plus de façon active, avoir des plans de surveillance actifs.

Sans une bonne surveillance, rien ne peut être effectué. Il faut faire attention à cela. Il y a quatre mesures dont je veux parler. Chaque compte bancaire, chaque propriétaire de compte bancaire a un genre de comportement qui est enregistré. Au Nigeria, cela donne une solution pour surveiller et voir ce qui se passe au niveau du comportement pour pouvoir facilement détecter s'il y a des escrocs qui prennent de l'argent dans des comptes multiples. Finalement, je suis content de ce que Jami dit dans ce contexte; il faut avoir beaucoup d'activités de façon délibérée et surveiller ces escrocs pour avoir où ils se trouvent et il faut les poursuivre au niveau juridique. Il faut que les escrocs sachent qu'ils seront attrapés et arrêtés. Il nous faut en faire plus à ce niveau.

>>BILEL JAMOUSSI : Merci. Il y a beaucoup d'éléments de la réglementation, deuxièmement c'est l'éducation du consommateur et troisièmement le partage des informations. Au niveau national comme Niyi Ajao l'a dit au niveau du Nigeria ou au niveau international comme Mohammed l'a mentionné pour pouvoir partager les informations en temps réel et agir rapidement. Vous avez mentionné la poursuite et la surveillance pour que les escrocs soient arrêtés et punis. Merci pour tout. Je vais maintenant ouvrir le micro à nos questions des participants. Une question adressée à tous les experts : À votre avis, est-ce qu'on s'attend à ce que les tendances émergentes prennent place dans les centres financiers et si oui ou non pouvez-vous exprimer votre opinion sur comment les tendances émergentes nous devons nous attendre à quelles tendances émergentes en particulier dans les ML et FT?

>>MERCY BUKU : Je vais y répondre. Pour le blanchiment d'argent, je dirai que les services de la fraude liée aux services numériques c'est un crime financier tout d'abord. On peut s'attendre à ce qu'il

se passe ; Mohammed a parlé des millions de dollars qui sont perdus dans les fraudes en cours. Et ce n'est pas nécessairement lié à la COVID-19. On peut s'attendre à de mêmes tendances dans les centres financiers comme Mohammed a donné un bon exemple. C'est déjà une tendance mondiale. Une fois que l'argent a été fait, c'est sûr qu'ils vont y trouver des façons de le blanchir. C'est là où nous voyons que les fournisseurs doivent surveiller les opérations pour qu'ils puissent aussi attraper les escrocs et s'assurer qu'ils ne leur permettent pas de se servir de leur plateforme de services financiers pour blanchir les gains criminels. Je réponds oui à cette question et cela a un lien direct au blanchiment d'argent. Je peux ajouter que les terroristes font du crime organisé et ce genre de fraude numérique en fait partie. Il nous faut donc aussi surveiller cela. Merci.

>>BILEL JAMOUSSI : Merci, Mercy.

>>MOHAMMED IMRAN : Je voulais ajouter à ce que dit Mercy. Le blanchiment d'argent est vraiment réel et les centres financiers en sont conscients. J'aimerais souligner à nouveau que cela est susceptible de se passer et c'est là où il nous faut une plateforme. Comme j'ai mentionné les différentes initiatives, elles ont été très efficaces pour nous aider à arrêter ou interrompre que les fonds atteignent les mains des criminels. Pour répondre en court, premièrement le blanchiment d'argent va être en augmentation dès que la COVID-19 est terminée et deuxièmement ce sera encore plus présent et il faudra faire des mesures supplémentaires comme je l'ai mentionné.

>>BILEL JAMOUSSI : Merci, Mohammed. Est-ce que d'autres membres voudraient répondre ?

>>JAMI SOLLI : J'aimerais répondre sur la question des victimes et leur vulnérabilité. Quand nous voyons que les personnes sont vulnérables, elles deviennent désespérées et à ce moment elles prennent des risques. Les gens feront n'importe quoi pour s'assurer qu'ils ne sont pas roulés. Oui, on va voir une augmentation de cela et il n'y

a pas de raison que ce ne soit pas le cas parce que les chiffres continuent à augmenter.

>>BILEL JAMOUSSI : Niyi ?

>>NIYI AJAO : Je voulais ajouter sur ce qui vient d'être dit. Je crois que la tendance va se poursuivre, c'est sûr. Tant qu'il y a des différences de distribution des revenus comme il y a un haut niveau de chômage au niveau mondial et que les limites de tout le monde sont très étroites, je crois que tout le monde dans l'écosystème, dans les services, dans les gouvernements, les régulateurs de la loi doivent s'assurer que ce soit arrêté.

>>BILEL JAMOUSSI : Une minute pour dire quelque chose en clôture ? Est-ce que les membres du panel veulent dire un mot de conclusion ?

>>NIYI AJAO : Je vais aller en premier. Je veux remercier l'UIT de ses efforts dans ce domaine. Il faut prendre les mesures adéquates pour faire face à cette escroquerie pour pouvoir minimiser l'impact de cette affaire. Nous devons continuer à nous assurer que les consommateurs sont protégés.

>>MERCY BUKU : Pour moi, j'aimerais dire que les régulateurs et tous les pays ont leur propre expérience. Mais en tant que régulateur et fournisseur, au fur et à mesure que les régulateurs et les fournisseurs continuent le statu quo il faut aussi protéger les consommateurs dont vous vous attendez qu'ils se servent de ces services financiers. On ne peut pas souligner cela plus qu'on ne l'a déjà fait aujourd'hui, mais les régulateurs et les fournisseurs doivent s'assurer de la protection de leurs consommateurs et des commerces.

>>BILEL JAMOUSSI : Merci, Mercy. Jami?

>>JAMI SOLLI : Merci beaucoup d'avoir organisé cet événement. Je crois que nous pouvons continuer à collaborer à ce sujet. C'est un très bon début. Nous avons beaucoup à faire, mais c'est un très bon commencement.

>>BILEL JAMOUSSI : Merci, Jami. Mohammed.

>>MOHAMMED IMRAN : Depuis INTERPOL, nous apprécions beaucoup l'initiative de l'UIT pour partager notre réflexion à ce sujet sur cette plateforme. Je peux répéter qu'il faut être proactifs pour faire des campagnes de sensibilisation et toutes les parties prenantes en font partie, s'impliquent. Il faut d'abord essayer d'interrompre ces transactions, trouver les escrocs. Et lorsqu'un crime se passe dans un endroit, il faut s'assurer qu'ils ne s'étendent pas rapidement à un autre endroit.

>>BILEL JAMOUSSI : Merci.

>>MERCY BUKU : J'ai oublié de remercie l'UIT d'avoir organisé ceci. Et même les webinaires précédents qui ont été très intéressants. Merci de m'avoir permis de présenter en tant que membre du groupe d'expert et merci aussi à mes autres collègues dans ce groupe d'experts. Cela a été très intéressant d'apprendre ce qui se passe dans les autres pays.

>>BILEL JAMOUSSI : Merci au groupe de travail d'avoir partagé vos réflexions sur ce sujet. Pour certains d'entre vous, depuis six ans, Jami, depuis ta première intervention dans le groupe de travail de DHF en 2014, merci de ton implication continue à l'UIT et d'avoir partagé ton expertise. Merci à Vijay et à l'équipe de l'UIT qui a rendu cette série de webinaires possible. Vijay, Arnold, Gifty et beaucoup d'autres qui ont mis beaucoup d'efforts pour apporter cette série de webinaires. Je veux reconnaître vos efforts à ce sujet. Je souhaite à vous inviter à notre prochain épisode qui se passera le 10 juillet. Nous allons suivre la discussion des crimes et des escroqueries numériques et nous fournirons des réflexions sur les outils qui peuvent être utilisés par les régulateurs et les agences d'application juridique pour surveiller ces activités frauduleuses. Merci à tous pour votre participation. Bonne journée ou bonne soirée et avant de fermer totalement, je vais mettre sur l'écran la participation à la série des webinaires en cette fin de mois de juin pour les séries qui vont commencer en juillet. Nous avons eu un total de sept épisodes avec 852 participants, 482

participants uniques et 94 pays participants. Merci à tous les membres du panel et à tous les participants. Nous nous réjouissons de discussions et de réunions à l’avenir dans notre prochain épisode. Sur ce, je déclare ce webinaire terminé. Merci.