FICHIER NON ÉDITÉ COMPLÉTÉ

Webinaire # 9 — Dépistage des crimes et des fraudes financières numériques

UIT -- Genève

10 JUILLET 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, bonsoir et bienvenue à ce neuvième épisode des webinaires sur les services financiers numériques lors de la série de webinaires COVID-19. Nous espérons que vous tous êtes en bonne santé et en sécurité.

Je suis Bilel Jamoussi du Bureau de normalisation de l'UIT à Genève. C'est un privilège d'introduire le webinaire d'aujourd'hui dans le dépistage des crimes financiers et de la fraude pendant la COVID-19.

Avant d'introduire les intervenants, je vais vous donner des informations générales concernant la logistique du webinaire d'aujourd'hui. Nous avons à peu près 150 à 200 participants inscrits et actuellement en ligne nous en avons 157 actifs. Nous nous attendons

à ce que ce chiffre augmente.

Aujourd'hui, nous avons du sous-titrage en français pour le webinaire. Si vous voulez activer le sous-titrage, cliquez au bas de votre écran.

Toutes les questions des participants seront prises à la fin pendant la session de Q&R. Les participants peuvent soumettre leur question en tapant leur question dans la foire aux questions. Quand vous soumettez la question par le biais de la fenêtre des Q&R, nous vous invitons à taper le nom de l'intervenant auquel s'adresse la question et si votre question s'adresse à tout le monde, écrivez votre question directement. Le webinaire est enregistré et l'enregistrement sera affiché sur le site Web un peu plus tard.

Je vais introduire les intervenants : Alexander Resch de INTERPOL; Thomas Silkjær de xrplorer.com; Assaf Klinger de Vaulto, Jami Solli de GALA et Rafe Mazer de Innovations for Poverty Action, IPA.

Durant cet épisode, nous allons examiner les différents outils et les façons dont les crimes financiers numériques peuvent être repérés. En 2020, la pandémie de COVID-19 a retourné le terrain de jeu et cela a un impact sur les vecteurs d'attaque. Nous avons discuté des crimes et des escroqueries financières numériques lors du dernier webinaire. Si l'argent physique était protégé dans des coffres bancaires comment est-ce qu'on la protège au niveau numérique ? Il s'agit d'une question d'inclusion financière, car la réponse est particulièrement importante pour les clients à faible revenu. Dans les pays développés, c'est généralement le prestataire de services financiers qui est légalement responsable des frais de fraude et les rumeurs de fraude vécues par d'autres provoquent une méfiance à l'égard des SFN, en particulier chez les consommateurs à faible revenu.

Les partenaires chargés de l'application des lois, 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 la pandémie de COVID-19. La communauté doit reconnaître que les enquêtes sur les délits de la finance numérique sont différentes des enquêtes sur les types de délits traditionnels. Il ne s'agit pas simplement d'une question de capacité d'organismes d'application de la loi. Chaque victime, détenteur de données ou organisme d'enquête, qu'il s'agisse du secteur public ou privé fait partie d'un écosystème mondial de plus en plus connecté et interdépendant.

Les compétences, les capacités et les données nécessaires pour enquêter sont du domaine de l'entreprise. Il s'agit d'un type de criminalité qui opère à un rythme différent, et il est donc beaucoup plus nécessaire de travailler selon des cadres et des principes communs convenus au niveau mondial et à la vitesse d'Internet. Cela comprend l'incitation au partage des données et à la collaboration et à la définition de rôles et de conseils clairs pour tirer parti des capacités de chacun.

L'établissement de principes est de plus en plus important à une époque où les préoccupations concernant la vie privée, le partage des données et l'interprétation de la législation telle que le GDPR entravent par inadvertance le partage d'informations précieuses.

Les entreprises détiennent souvent des données critiques, mais ne se sentent pas en mesure de les partager en raison de préoccupations concernant la confidentialité des données, la confidentialité des clients ou la divulgation de renseignements à des concurrents. Des nouveaux outils et plateformes utilisant des technologies teck le cryptage homomorphe seront nécessaires pour aider à construire des modèles plus durables pour protéger les victimes et permettre des enquêtes mondiales, tout en respectant le droit à la vie privée. L'établissement de principes de normes et d'harmonisation des cadres de cyber réponses entre les victimes, les prestataires de services financiers numériques les forces de l'ordre et les institutions

transnationales sont des exemples importants de la manière de réduire les marges de coopération dans lesquelles opèrent les cybercriminels. Nos panélistes vont fournir quelques exemples d'outils qui peuvent être utilisés pour les régulateurs pour repérer les crimes financiers numériques. Maintenant, il est temps de se tourner vers nos panélistes. Le premier conférencier est Alexander Resch. Vous avez la parole pour 15 minutes, s'il vous plaît.

>>ALEXANDER RESCH : Merci. Bonjour, bonsoir. En fonction de là où vous vous trouvez. D'abord, merci à l'UIT de m'avoir invité et mes collègues de prendre le temps en ce vendredi pour écouter ce sujet intéressant. Je suis Alexander Resch et je suis un agent de police de INTERPOL et nous avons notre siège social en France et pendant les prochains 15 minutes je vais introduire les crimes numériques et ce que fait INTERPOL pour aider les forces de l'ordre dans les 95 pays ce que nous desservons.

J'aimerais d'abord vous amener en petit voyage dans l'environnement des crimes numériques qui est très vaste. Puisque nous avons des participants du maintien de l'ordre public, mais aussi des institutions financières, de la banque centrale, et cetera, je crois que beaucoup d'entre vous connaissent déjà ce genre d'escroquerie et de fraude. Pourtant, j'aimerais souligner et me concentrer sur certains d'entre eux parce que ce sont des phénomènes et des facettes des fraudes numériques qui ont un impact sur tout le monde : les gouvernements, les individus et les entreprises. Et en même temps, une fois qu'on rapporte cela à la police, ils font des enquêtes sur le terrain et ils gardent nos collègues très occupés parce que nous voulons amener les criminels à comparaître devant la justice et subir la peine pour leur crime.

Ici, vous voyez quelques-uns des exemples des crimes financiers de la fraude numérique, mais il y en a bien plus. Je vais me concentrer sur — ils ont commencé à cibler des entreprises en France et maintenant c'est une pandémie mondiale. Nous voyons partout dans le monde et c'est

un business de multimilliardaires pour les criminels qui volent des entreprises pour des milliers de dollars. Une fois l'argent transféré dans des comptes bancaires, ce n'est pas difficile pour eux d'obtenir l'argent, mais c'est difficile pour les gens du maintien de l'ordre d'enquêter ce genre de crimes. C'est un défi en croissance. Concernant les fraudes en ligne, dans certains pays cela s'appelle aussi les cyber échanges. Je vois des possibilités numériques en ligne. Ils mettent en place des sites Web faux en faisant semblant d'être des compagnies réelles financières. Ils font semblant de faire des gains très rapides. Nous avons ce genre d'accident partout dans le monde ; ces escroqueries en ligne qui ont un impact sur beaucoup de victimes. C'est une grande occasion pour que les criminels gagnent énormément d'argent et qu'ils puissent ne pas se faire attraper.

Pas seulement — l'argent, une fois volé, doit être blanchi par le biais des institutions financières et sous d'autres formes. Nous avons aussi des systèmes de transfert qui sont comme Hawala qui est un outil spécifique pour le blanchiment d'argent par les criminels et cela garde nos collègues très occupés sur le terrain parce qu'il y a une croissance de ce genre d'activité dans certains pays et les personnes font partie d'affaires criminelles, reçoivent des fonds volés et les blanchissent pour des criminels. C'est un genre de mule. Ce qu'on fait parfois, pendant la pandémie, comme nous l'avons dit, nous avons vu des phénomènes de crime financier facilité par la COVID-19. Nous voyons du blanchiment d'argent basé sur l'ethnie pendant la pandémie ; nous avons des phénomènes de crimes très attrayants pour les groupes du crime organisé. On va se concentrer sur les escroqueries que livraison ; par exemple, nous avons des cas qui ont commencé en janvier en Asie en raison du manque de masques et de respirateur nous avons vu des criminels qui établissent des sites Web de fraude faisant semblant qu'ils sont fabricant et qui collectent l'argent des victimes qui veulent acheter ce genre de masque et qui ne les reçoivent bien entendu jamais. Ce

phénomène est encore en place à l'heure actuelle et nous voyons encore ce genre de faux site Web et des publicités en ligne et les criminels font semblant qu'ils vont vous livrer ce genre d'équipement de protection personnel et ils ne sont bien entendu jamais livrés. Dans cet exemple, nous voyons ce genre d'escroquerie seulement fait par des groupes ethniques, pas seulement pour mettre en place la fraude, mais pour dominer aussi les activités de blanchiment d'argent et de façon intéressante ces cas pas simplement le genre d'escroquerie et les activités sont dominés par des groupes ethniques spécifiques.

La réalité actuelle, nous avons un seul acteur, il est très impliqué pour faire un compromis et faire ce genre d'escroquerie de chez lui. Dans beaucoup de pays, pas toutes les victimes ciblées ont reçu ce genre de courriel sont devenues des victimes. Cependant, il y a un petit pourcentage dans des compagnies ou des entreprises qui sont devenues des victimes ; ils ont transféré des fonds et avoir un seul acteur qui cible des victimes dans beaucoup de pays, du point de vue du maintien de l'ordre public, nous avons des rapports de victimes faits à des membres de la police par des victimes dans beaucoup de pays. Tandis que les suspects opèrent d'un autre pays. Vous avez beaucoup de pays et de force de maintien de l'ordre public qui sont impliqués dans beaucoup de pays. Beaucoup de ces connexions et les enquêtes qui sont menées par les forces de l'ordre public ne sont pas interconnectées entre les pays, mais elles devraient l'être pour que les polices des pays différents puissent échanger les informations pour pouvoir faire face à ce genre de crime et les amener, les faire comparaître devant la justice. Les défis actuels, c'est là où INTERPOL intervient, c'est de connecter toutes les polices des différents partis pour qu'ils puissent collaborer dans les enquêtes. C'est un exemple, cette diapositive, d'un crime financier concernant des fraudes de télécommunications. Le crime téléphonique est conduit par coup de fil, mais en ce qui concerne les activités de blanchiment d'argent, les victimes qui ont été roulées par téléphone, ils font une opération pour

un compte bancaire à l'étranger sous le contrôle d'un criminel. Il s'agit ici d'une approche intéressante avec la police de l'Inde. Ils ont fait une enquête et arrêté les criminels et ont vu que les criminels ont déterminé que les personnes qui ont fait les appels n'étaient pas en Inde, mais au Royaume-Uni ou en Australie. Pour pouvoir bâtir le cas et continuer l'enquête et faire comparaître les criminels devant la justice, ils se sont fiés aux déclarations des victimes. Et là, ils ont choisi une façon spécifique de faire appel à différentes ressources. Ils ont appelé les victimes pour qu'ils se mettent en contact avec les enquêteurs de l'Inde par courriel pour soumettre leur plainte pour que la police puisse mener l'enquête. C'est une méthode spécifique qu'on n'a pas vue souvent, mais c'est pour vous donner une idée de comment la police doit gérer la situation. Pour présenter un bon cas, des preuves au tribunal pour pouvoir faire arrêter les criminels. Parce que souvent, il y a des défis du point de vue du maintien de l'ordre public, les personnes dans les pays différents, amener les dossiers et les informations pour que le criminel soit amené devant la justice dans le pays approprié.

Les forces de la police dans beaucoup de pays par le passé ont commencé à offrir des ressources en ligne où le crime peut être rapporté en ligne. Ces signes ne sont pas seulement des outils pour rapporter les crimes en ligne pour les victimes, mais c'est aussi possible que les personnes à l'étranger puissent signaler des crimes dans des pays spécifiques. Par exemple, au Royaume-Uni, qui se trouve à gauche, ils ont mis sur place un site de fraude d'action où les cybercrimes peuvent être rapportés par les gens du Royaume-Uni et aussi par les gens à l'étranger. Même si l'enquête ne mène à rien, on peut examiner les activités de blanchiment d'argent. De façon similaire, il y a eu le site de SDCC qui est aussi un site Web très intéressant mis en place par la police de Hong Kong et ce sont deux bons exemples. Le rôle de INTERPOL dans 194 pays membres c'est de connecter tous les collègues sur le terrain pour qu'ils puissent partager les informations les uns

avec les autres. Dans le cadre de ce réseau qui connecte les forces du maintien de l'ordre public, du point de vue de INTERPOL, nous n'avons pas un mandat de faire, mais nous voulons aider les membres du maintien de l'ordre public pour faire leur travail et échanger les informations partout à l'étranger pour ajouter de la valeur à leurs enquêtes et interconnecter les cas. Avant de finir ma présentation, dans la dernière diapositive, c'est une étude de cas et un exemple qui concerne un crime que nous avons vu, une fraude que nous avons vue dans les dernières semaines et mois qui s'appelle Plus token. Des centaines de victimes dans la région asiatique ont été volées et en ce qui concerne des avertissements de cryptomonnaie et nous avons vu aussi là-dessus que les criminels ont obtenu des fonds d'investissement de cryptomonnaie et ont démuni les victimes d'énormément d'argent. À l'heure actuelle, vous avez des pays multiples et des agences de maintien de l'ordre public qui sont impliqués dans des enquêtes et vous voyez les suspects dans cet exemple ici, ils sont de Chine et ils ont été arrêtés au Vanuatu et les victimes de beaucoup de pays pas seulement dans la région asiatique, mais aussi en Europe et d'autres pays du monde. En ce qui concerne la recherche des fonds blanchis et repérer toutes ces activités, les personnes disons qui sont inscrites en Afrique, par exemple, dans certains cas, des forces de maintien de l'ordre public sont dans beaucoup de pays et les enquêtes doivent être interconnectées pour que la police puisse collaborer pour pouvoir réunir les informations et présenter un bon cas auprès du tribunal. Je crois aussi que je viens de finir ma présentation. J'espère que cela a aidé à vous donner une idée du travail de INTERPOL et des défis des forces de l'ordre et merci de votre attention et j'attends vos questions à la fin du webinaire.

>>BILEL JAMOUSSI : Merci de cette présentation très claire sur le rôle de la fraude et votre rôle dans les 194 pays où INTERPOL opère pour faire face aux crimes qui dépassent les frontières d'un pays et permettre la collaboration des forces de la police au niveau

international. Tu as montré des exemples d'outils en ligne que la police et d'autres centres utilisent pour rapporter ces crimes internationaux et y faire face de façon efficace. Merci beaucoup. Nous allons revenir vers toi plus tard.

Maintenant, je passe à Thomas Silkjær pour qu'il nous donne sa présentation à ce sujet. Thomas, pour 15 minutes.

>>THOMAS SILKJAER : Merci. Bonjour, bonsoir à tout le monde. Je suis Thomas Silkjær et je suis le fondateur de xrplorer.com. C'est une compagnie qui a fait des enquêtes dans les biens numériques. On nous dit souvent que blockchain et la cryptomonnaie facilite la situation pour que les criminels volent des fonds et le blanchiment d'argent sans être attrapés. En considérant que la plupart des biens numériques sont mutables, persistant, il est possible que ce soit l'opposé et que cela rende cela très difficile pour les criminels de blanchir l'argent. Notre spécialiste, quand quelqu'un envoie un paiement, cela se passe de façon très publique. L'opération entière est publique et le registre des transactions est public dans n'importe quel compte. Cette activité des comptes qui envoie et reçoit des paiements est facile à repérer où les paiements sont visualisés par des flèches qui connectent les points. Chez xrplorer.com on maintient ce graphique d'abord base de données ; c'est une représentation de l'historique complet de toutes les activités qui rend possible un travail efficace avec un montant énorme de données qui se passent en temps réel. Avec près d'un million d'opérations, cela se traduit en une base de données immense. Mais quoique le registre soit transparent et tout ce qui se passe dans les cryptomonnaie soit public, cela n'a pas de lien à part du compte sur la blockchain pour les entités réelles et sans savoir qui se trouve derrière le compte, la transparence n'est pas d'une grande aide en ce qui concerne le combat contre les crimes financiers numériques. C'est la raison pour laquelle dans notre base de données nous avons ajouté des renseignements réunis sur un compte comme le fournisseur de service virtuel où on peut acheter des cryptomonnaies, mais aussi en ce qui

concerne les comptes impliqués dans des activités criminelles. Avec cette intelligence ajoutée concernant les comptes individuels du réseau, nous pouvons travailler avec des algorithmes pour trouver des grappes de comptes pour pouvoir localiser les activités criminelles. Cela pourra nous aider à identifier des comptes qui y sont liés les uns avec les autres dans les activités criminelles.

En ce qui concerne l'intelligence, nous avons appris de plus en plus concernant les comptes qui interagissent sur la blockchain ou le registre. Cela révèle aussi pourquoi la blockchain est une mauvaise nouvelle pour les criminels, parce que la technologie transparente laisse des traces permanentes qu'on ne peut pas effacer. Lorsqu'on reçoit un rapport d'escroquerie, on ajoute cette intelligence à la base de données qui desserve des objectifs variés pour fournir une liste de conseils pour les fournisseurs de services pour qu'ils puissent saisir et rapporter les paiements reçus de ces comptes frauduleux. Il peut aussi identifier les comptes qui y sont associés y compris regrouper les cas présents à ceux passés et les lier par les regroupements de comptes et on peut contacter les fournisseurs de bien susceptibles de recevoir des fonds blanchis sur la base de l'historique des comptes en banque regroupés. Alexander a parlé de cela et c'est très bien ; il y a des victimes dans des pays multiples. C'est très difficile de savoir quelle force de maintien de l'ordre joindre ; la plupart du temps si on travaille avec la police dans le pays en question où s'est passée la fraude, c'est ce qu'on fait d'habitude. Je vais partager quelques exemples sur comment les activités illicites peuvent se manifester. Lorsque vous regardez le graphique et lorsque vous combinez les activités du passé avec une surveillance en temps réel ; comme Alexander l'a dit dans la présentation précédente, il y a eu un programme d'investissement très lucratif qui a été présent en 2018 ou 2019. Cela donne l'illusion d'investir dans une entreprise durable et référer des amis et de la famille et beaucoup de personnes ont été

victimes de cette fraude. En juin 2019, des utilisateurs ont eu des retards quand ils ont essayé de retirer les fonds, mais cela s'est arrêté de façon abrupte le 30 juin 2019 quand tous les paiements d'intérêt ont cessé et cela a été confirmé par la suite par des mouvements de grandes sommes d'argent depuis ce site frauduleux suivi par des avis disant désolé, nous sommes partis et tout le monde savait qu'ils ne verraient plus jamais leur argent. Selon plusieurs sources, cette fraude a réussi à voler 3 milliards de dollars. Quand un compte a commencé à bouger des fonds à peu près il y a un mois, un an après la fin de ce complot, nous avons commencé à enquêter à savoir comment connecter les comptes passés aux comptes actuels. Cela, c'est ce qui se passe sur cette diapositive. Vous avez les fournisseurs de services publics et si vous voyez ma souris, les points orange sont les fournisseurs de services externes utilisés pour le blanchiment d'argent dans le cadre de ce complot. Il y a de l'argent qui arrive émanant des fournisseurs de service virtuel. La grande masse du milieu, il y a sept ou 8000 comptes différents utilisés pour remuer l'argent de part et d'autre. Plus de 100 000 paiements individuels pendant plus d'une année et ils ont remanié tous ces fonds et cela a été très difficile de les tracer et de savoir où ils allaient. Quand vous regardez, il y a en fait seulement des rentrées et c'est à peu près 5 millions du complot et il y en a quelques biens qui sont dirigés vers les personnes qui font le blanchiment d'argent.

Le remaniement des fonds et pendant le mois passé, il a envoyé plus de 3 millions ou presque 60 millions de dollars américains vers des fournisseurs de services virtuels.

Un autre exemple ici ; comment se servir de la surveillance en temps réel de l'argent ; ce sont des exemples d'hameçonnage et cela a alerté la personne qui recevait le message de saisir leurs informations bancaires en leur promettant des grands bénéfices. Après avoir acquis les informations des comptes bancaires, les comptes ont été vidés un

par un. Ce graphique visualise ces activités. En bleu clair, ce sont les comptes qui sont utilisés pour envoyer les micro-opérations et les comptes qui sont soulignés en violet se trouvent et sur le périmètre sont les comptes utilisés pour vider les comptes des victimes et les victimes sont en vert. Tous ces comptes en vert, il y a beaucoup de comptes où les victimes ont perdu tous leurs fonds. Un par un, les fonds ont été déplacés par des comptes tout nouveaux colorés en jaune, souvent par chaînes pour effacer la trace d'une façon ou d'une autre et les déplacer pour être blanchis. Merci. La plupart des actifs numériques sont exploités par des blockchains où l'historique ne sera pas effacé. Les traces vont rester. Les bons outils à combiner l'intelligence du passé à celle du présent peuvent aider à empêcher les crimes financiers. Avec des partenariats avec le secteur public et privé pour fournir des outils aux forces de l'ordre, cela peut restreindre ce genre d'activités.

>>BILEL JAMOUSSI : Thomas, c'était fascinant ; merci beaucoup. Comme certaines des propriétés qui sont utilisées par les blockchains pour blanchir l'argent, ces mêmes propriétés ont été utilisées au niveau mondial pour tracer cet argent qui découle de ces complots financiers énormes. Tu as mentionné 3 milliards de dollars qui ont été perdus ou volé à travers ce complot. Fascinant ; merci beaucoup, Thomas. C'est vraiment super que ta présentation ait été complémentaire à celle de Alexander Resch de INTERPOL. Je vais passer maintenant à notre prochain intervenant, Assaf Klinger qui nous vient de Vaulto. Merci beaucoup, tu as un quart d'heure.

>>ASSAF KLINGER : Merci beaucoup de m'avoir invité aujourd'hui. Ma présentation est un ajout à la présentation de mon collègue comment tout le monde ou les personnes du maintien de l'ordre public ou si vous êtes une victime, comment vous servir des outils gratuits sur Internet pour pouvoir, disons, repérer les fonds qui ont été volés. D'abord, je vais vous parler de moi-même. Je suis un chercheur financier depuis

18 ans, j'ai travaillé sur beaucoup de cas en Israël. C'est mon pays natal. Je fais partie des forces de maintien de l'ordre public et nous avons détecté une grande opération de drogue qui a bougé l'argent d'ici et là. Et pour ne pas répéter ce qu'ont dit les autres, la cryptomonnaie est une alternative au système financier réglementaire et se servir de la cryptomonnaie est très pratique pour les criminels parce qu'ils peuvent faire ce qu'ils veulent avec l'argent. Les escroqueries de cryptomonnaie sont d'habitude bâties comme des arbres et les complexes sont comme des graphiques. Si vous regardez de plus près l'arbre, c'est ce que j'appelle le portefeuille public. C'est l'argent que la victime a transféré et après l'argent devient envoyé par une chaîne de portefeuilles frauduleux dans le portefeuille racine là où l'argent est blanchi.

La première étape pour pouvoir repérer la fraude, c'est de faire une enquête, que ce soit au niveau personnel ou que vous ayez été victime d'une escroquerie en ligne. Il y a aussi des sites Web où les gens rapportent les escroqueries où les membres du maintien de l'ordre public au niveau local ont leur propre force d'enquête. Ce sont deux sites générés par la communauté et ils sont publics et gratuits. Si vous regardez une escroquerie simple, comme je l'ai dit cela commence du portefeuille public ; ce que vous voyez sur le site, WhatsApp ou autre, l'argent est ensuite déplacé au portefeuille racine. Qu'est-ce qui se passe ; comment l'argent en ressort ? Les complications de l'arbre simple ou de l'escroquerie par cryptomonnaie. D'abord, ce sont les piscines d'échange, le portefeuille racine est échangé et l'argent est échangé vers des groupes, des bassins de fonds énormes et on ne peut pas les différencier des autres fonds. Ils obtiennent l'argent et les escrocs font des échanges internes et après ils prennent l'argent et le dirigent vers une autre forme de cryptomonnaie et par des devises entre les dollars et les euros et ce mouvement est simplement repéré dans la base de données.

Une autre complication en ce qui concerne le repérage des cryptomonnaie, vous avez le bitcoin et d'autres registres. Il y a la possibilité de faire beaucoup de transactions de beaucoup à beaucoup. Dans ce cas-là, vous avez beaucoup d'entrées et de sorties et le graphique des opérations n'est pas seulement deux points et une flèche, mais 100 points et flèches allant vers 70 points et flèches. On ne sait pas qui est quoi. Il y a l'échange des jetons, un saut de blockchain qui dit qu'il vient de ramener un portefeuille racine, beaucoup de cryptomonnaie et je veux que ce soit non traçable. Je veux le faire disparaître. Qu'est-ce que je fais ? Je prends une victime et je lui dis, j'ai des bitcoins. Toi tu as Ethereum, on fait l'échange. Le jeton frauduleux qui a été pris est vendu, que ce soit à une police ou à une victime innocente qui croit faire un échange légitime. En retour, le fraudeur obtient un jeton propre dans sa blockchain et qui n'est pas traçable à un certain degré. Là, ce sont les complications de cet arbre simple. Je passe à quelque chose d'autre maintenant.

Je commence à surveiller cela quand j'ai — je m'arrête. La fin du processus de repérage. La difficulté, c'est d'attribuer un nom, une personne, qui est le propriétaire de ce portefeuille racine ? Comment est-ce que je peux avoir un nom, un numéro de téléphone, une adresse courriel et deuxièmement là où j'arrête le repérage, c'est là où j'ai un bassin d'échange et on peut se fier au fait que les fonds sont bien arrivés. Voici un exemple. Voici une escroquerie qui s'appelle un Ponzi. Alors voilà, il y a un investissement factice à haut bénéfice et bien sûr les personnes veulent investir, mais c'est un Ponzi, une escroquerie. Voyons voir les finances ; quand vous regardez le portefeuille affiché sur le site Web, vous voyez des dépôts et à gauche en vert vous avez les victimes et parfois une fois par jour, les escrocs prennent tout l'argent et le sorte et vous voyez le solde du portefeuille qui est de zéro et c'est caractéristique des portefeuilles, feuille. On continue. Cela, c'est un portefeuille très

actif et occupé en mars 2019 qui a fait des opérations de 14 000 $, mais c'est seulement une seule feuille de l'année précédente. Il y a aussi une exfiltration directe de 600 000 $ américain fait par les victimes et cela a été déplacé vers des sites qui sont des points d'échange. 75 % des fonds ont été envoyés vers le portefeuille de canalisation. Le portefeuille de canalisation a reçu des fonds et les sorts, les faits sortir. Vous voyez le site de canalisation. En bas, vous avez les dépôts et ils ont été sortis et le solde en est à zéro. Un autre dépôt et une autre exfiltration et une autre canalisation. Cela, c'est le cycle de la canalisation. Ce portefeuille de canalisation en particulier a eu 46 opérations et 12 cycles de canalisation. Beaucoup de gros montants ont été canalisés vers ces portefeuilles ici. Le premier est un portefeuille de canalisation qui est là, difficile à tracer, mais qui ne masque pas tout. Le premier c'est la racine, depuis ce portefeuille racine, les fonds ont été échangés par les euros et les dollars américains. C'est un portefeuille brûlant qui exfiltre les fonds vers un site en Chine. Ce portefeuille travaille en tandem avec beaucoup d'autres portefeuilles. Ce sont des grandes escroqueries et ce n'est pas très lucratif et n'a pas beaucoup de bénéfice. C'est seulement un exemple. Il a généré plus de 138 millions de dollars américains. C'est encore un portefeuille qui a volé 19 000 bitcoins et cela c'est un portefeuille que cela vaut la peine de poursuivre parce que l'argent s'y trouve encore. Qu'est-ce qui vient maintenant après ? Vous pouvez prendre cela et le développer. Mais de façon plus importante, il faut commencer à parler aux forces du maintien de l'ordre public pour réunir, parce que trouver les numéros de téléphone et les courriels c'est très difficile et c'est l'affaire, le domaine des membres du maintien de l'ordre public. De nos jours, quand les membres du maintien de l'ordre public ouvrent, vont connecter des fournisseurs de services financiers et qu'ils leur parlent de l'argent transféré dans leur compte, veuillez me donner le nom du propriétaire du compte bancaire et qui a reçu ces

fonds et c'est là que vous obtenez le nom ou le courriel ou le numéro de téléphone ou l'adresse physique associés avec un portefeuille de cryptomonnaie anonyme. J'attends vos questions après le webinaire. Merci.

>>BILEL JAMOUSSI : Merci beaucoup, Assaf. Cela a été fascinant. J'ai retenu les portefeuilles, feuille, les portefeuilles racine. C'est comme cela que le complot Ponzi a commencé quand ils se sont fiés au portefeuille public et pour le déplacer par cette chaîne de canalisation et tu as mentionné les complications inhérentes aux regroupements de fonds et aussi au repérage des crimes et des comptes en se fiant au KYC qui a ouvert ce genre de compte. Merci beaucoup, Assaf. On va revenir vers toi avec des questions plus tard.

Maintenant, je passe à Madame Jami Solli. Vous avez un quart d'heure.

>>JAMI SOLLI : Merci, Bilel et merci à l'équipe de l'UIT d'avoir organisé tout cela.

Vous pouvez voir mon écran.

>>BILEL JAMOUSSI : Non, pas encore.

>>JAMI SOLLI : Comme vous pouvez le voir, je vais parler des outils de prévention. On a entendu parler de comment surveiller, repérer. Mais moi j'ai pris des titres d'articles de journaux retrouvés partout dans le monde et il y a des énormes montants d'argent volé et très rarement recouvrés. On prédit que plus haut niveau de complot Ponzi va se passer dans un avenir proche. Pour pouvoir surveiller une autre menace de Chine Ponzi, la police a essayé de recouvrir les 27 millions de dollars volés, mais c'est rare. Nous pouvons nous concentrer mieux sur ces outils pour pouvoir empêcher les crimes et économiser les fonds du grand public et le traumatisme qui y est associé. Je vais parler un peu de moi et de UDIS. Bilel et Vijay savent que cela m'intéresse énormément et cela découle de mon travail pour l'intérêt public. Je suis une avocate de la protection des consommateurs et depuis dix ans je suis consultante indépendante sur la protection des consommateurs financiers. Il y a beaucoup d'exemples de complots très basiques et très évidents, mais

d'une façon ou d'une autre les personnes sont des victimes quand même. J'ai aussi un organisme à but non lucratif qui s'appelle GALA pour aider les victimes. En 2014, nous avons moi et d'autres avocats examinés un complot qui se passait en Ouganda qui voulait s'occuper des veufs et des orphelins partout dans le monde et se sont servis de personnes connectées au niveau social pour leur dire d'investir en fait dans un complot Ponzi. Lorsque nous avons regardé les prêts faits par les victimes, une fois l'enquête faite, tous les fonds avaient déjà été écoulés et nous ne pouvions rien faire. Nous leur avons dit que tout ce que nous pouvions faire était de partager leur histoire. Nous avons interviewé les personnes, j'ai parlé à des personnes qui avaient perdu leur femme ou mari en raison de suicide, les grands-mères qui se retrouver SDF dans la rue et j'ai mis tout cela sur un site Web public dans le cadre d'un article du quotidien *Guardian*. Il y a eu des enquêtes au Kenya, Inde, Bangladesh et Nigeria. Il y avait beaucoup d'agences qui avaient le mandat de prendre des actions policières, mais on a trouvé qu'il n'y avait pas beaucoup de collaboration. Il y avait trois ou quatre agences, mais ils ne partageaient pas l'information de façon efficace et il n'y avait pas de prévention au niveau du maintien de l'ordre public. Un seul cas où la victime a été remboursée. Nous avons eu la chance de trouver des données intéressantes par le biais d'une banque et ils ont vu un crime en progrès, c'est le MMM qui a commencé en Russie dans les années 90 par un criminel célèbre et ce complot a été copié et en ligne il y avait un cours en ligne pour comment enseigner les complots Ponzi. On a vu pendant six mois un seul complot a volé plus de 70 millions de dollars américains à partir du Nigeria. Ces 70 millions de dollars c'est plus que tout le budget d'éducation nationale du pays du Nigeria. C'est un immense complot, donc. C'est au niveau macro. Nous avons affiché notre rapport et complété l'enquête en 2017 et nous travaillons sur comment piloter des recommandations ; nous avons 13 recommandations concernant les meilleures collaborations et vous pouvez le lire en ligne. Les recommandations au niveau national

et international pour obtenir une collaboration efficace et les intervenants précédents en ont parlé.

En gros, je crois qu'il faut avoir une plus grande concentration sur les réseaux sociaux et l'implication de ces réseaux sociaux. Il est impossible de faire le complot sans les réseaux sociaux. Dans l'ancien temps, tout le monde se rencontrait face à face ou s'appelait et pouvait se convaincre les uns et les autres de faire cela. Maintenant, tout se passe sur les réseaux sociaux, Facebook, YouTube, et cetera. On voit que dans les modalités de Facebook, on dit que ce genre de publicité est signalé par Facebook en disant que c'est une fraude, nous allons les descendre, mais en fait Facebook ne le fait pas. Je recommande que cela fasse pression sur les réseaux sociaux pour qu'ils vraiment mettent en application leur menace. La prévention et aussi la surveillance et l'identification de UDIS. La recherche a émané de l'université en Italie et ils ont réussi à détecter des complots Ponzi et l'ont fait comme cela ; ils ont d'abord identifié un complot Ponzi en cours. Ils ont regardé le MMM et comparé le code-barre avec celui d'un complot Ponzi connu et ont regardé la différence des caractères. Et si vous voyez des différences de caractère dans ces byte code ce n'est probablement pas un Ponzi, mais s'il y a très peu de différences, c'est probablement un Ponzi. Il y a eu aussi une surveillance continue des opérations blockchains effectuées par un groupe mélangé de Berkeley, Qatar et Luxembourg et de Sri Lanka. Ils ont considéré le complot MMM ; ils ont surveillé des bitcoins et tous les chats à ce sujet dans les forums et ils ont regardé des opérations. Ils ont regardé 420 000 conversations de ce genre pendant une certaine période de temps ; 41 % des participants n'ont pas reçu de retour de la coopération MMM. Un autre pourcentage assez bas a probablement été les personnes qui ont reçu un peu d'argent et après ont amené leurs contacts sociaux et elles étaient peut-être des victimes inconscientes ou des personnes qui ont permis à l'escroquerie de se propager. L'escroquerie a gagné

765 000 —

(Problème technique de son)

Ils vont peut-être aller dans la police locale ou auprès de militants pro consommateurs. On voit beaucoup d'implication de la part de la société civile et de sociétés de protection des consommateurs qui sont inondés de plaintes et en temps de COVID-19 ils les reçoivent par texte ou en ligne. Ces organismes sont inondés de demandes, de plainte : j'ai perdu mon argent et j'ai du mal à sortir mon argent de tel ou tel portefeuille. Ce serait donc une bonne occasion pour les régulateurs de réduire cet écart et aider les compare. J'ai trouvé une recherche intéressante à ce sujet et mon collègue va vous parler, Rafe il va parler des plaintes des consommateurs en ligne. En gros, je crois même que dans la discussion d'aujourd'hui il y a beaucoup d'outils en place et le grand problème est la collaboration pour le partage des données.

Nous n'avons pas raison de croire que les criminels vont s'arrêter ; ils sont complètement impliqués dans les activités et on ne sait même pas, dans le dernier rapport de 2019 il y avait 4,3 milliards de dollars qui émanait de l'escroquerie Ponzi principe à me — principalement. Merci à tous.

>>BILEL JAMOUSSI : Merci à toi. Je suis toujours très heureux de t'avoir dans nos webinaires. Merci beaucoup d'avoir partagé le complot en Ouganda, le complot MM même chose au Nigeria. Ta discussion des réseaux sociaux et ce qui se passe à ce niveau et les politiques des réseaux sociaux qui interdisent ce genre d'activité, mais qui ne les mettent pas à exécution.

Il faudrait les encourager à appliquer, à imposer leurs interdictions juridiques.

Voici maintenant Rafe Mazer qui vient de l'IPA. Et aussi Jami a parlé des sources où l'argent volé a été pris et comment l'argent a été blanchi. On la remercie et à nouveau nous repérons à Rafe, notre dernier intervenant, mais non pas le moindre, pour faire le suivi de ce qu'a

dit Jami.

>>RAFE MAZER : Merci beaucoup. Je vais afficher ma présentation. Voilà. Bonjour, je suis Rafe Mazer de la société de protection des consommateurs. Je vais parler un peu du côté de la vente au détail à laquelle les consommateurs font face. Les trois piliers de mon travail : l'innovation d'action d'innovation pour la pauvreté ; amener plus d'évidence en ce qui concerne les règlements pour réduire la pauvreté et la protection des consommateurs. En général, nous collaborons avec les gouvernements, avec les fournisseurs de prestations dans les marchés variés et nous les connectons avec les chercheurs pour créer des sondages et d'autres évaluations d'impact et nous lançons une nouvelle initiative de recherche de protection des consommateurs qui se trouve sur notre site Web si cela vous intéresse. Nous considérons aussi des collaborations sur les sujets actuels.

Donc, nous avons recherché, nous avons pris l'approche — je vais partager quelques-unes de nos activités. Nous avons développé des questions sur la COVID-19 et les problèmes de fraude. Nous avons des sondages de protection des consommateurs qui sont internationaux sur trois marchés. Nous sommes au Kenya, en Ouganda et bientôt au Nigeria et nous espérons au Bangladesh. Nous voulons voir de quelles fraudes spécifiques il s'agit, des escroqueries, de l'hameçonnage lié au COVID-19 et nous voulons voir s'il y a en particulier des escroqueries liées à la COVID-19. Cela a été demandé par les régulateurs au sein de ces pays parce qu'ils ont vu une croissance des problèmes liés aux escroqueries des consommateurs. Parce que, quand le gouvernement fait un paiement, un transfert de paiement social aux consommateurs au niveau de la COVID-19 ; on leur demande des informations bancaires et vous pouvez imaginer ce qui suit. On leur demande s'ils ont reçu des messages de ce genre et des coups de fil et ce qu'ils en ont fait. Est-ce qu'ils ont rapporté cela ? Une autre chose sur laquelle nous travaillons avec les régulateurs et qui est liée à la COVID-19, nous menons des

analyses, des rapports des consommateurs émanant des opérateurs et cela va aux fournisseurs. Ils ont reçu le coup de fil ou la demande d'aide de la part de ces consommateurs. Dans un marché, parce que, ce que nous faisons, nous considérons les rapports mensuels des consommateurs émanant de MNO, par exemple 100 000 dossiers et on peut mesurer par le nombre de plaintes et la catégorie. Et on peut, il y a beaucoup de logiciels de traitement nationaux pour traiter les impôts. Ce que nous faisons, c'est d'ajouter plus de variables pour apprendre. Les clients ne capturent pas toutes les données. Toutes ces données peuvent nous donner énormément pour savoir qui a été contacté et qui en souffre le plus. Nous pouvons après faire des campagnes de sensibilisation auprès des consommateurs. Un autre domaine que Jami a mentionné tourne autour de surveiller les médias sociaux pour repérer les escroqueries et les abus des consommateurs et les escroqueries liées à la COVID-19. Ce graphique que je vous montre est un exemple d'un pilote effectué au Kenya en 2019 où nous avons utilisé une plateforme d'analyse des médias sociaux pour comprendre quel est le volume compte tenu de la protection des consommateurs qui est ciblée sur les fournisseurs de services financiers, les banques, et cetera. Nous avons vu — nous avons testé des alertes et les fournisseurs se plaignent un peu plus de 10 % sur 30 jours, le régulateur peut recevoir un courriel et un avertissement. Au lieu d'avoir des données à la fin du mois, cela donne une surveillance des activités en temps réel. Nous prenons un plus grand échantillon du marché et on l'examine. Qu'est-ce que cela pourrait nous dire ? Nous espérons pouvoir nous servir de ces données en temps réel avec les régulateurs.

Pour conclure, du point de vue de la recherche, de notre côté à nous, il y a quatre messages sur lesquels il nous faut collaborer avec les fournisseurs pour faire face aux problèmes liés à la COVID-19 et autres problèmes des consommateurs.

D'abord, revoir les données administratives que vous possédez.

Souvent les gens collectent beaucoup de données et ne s'en servent pas ; est-ce qu'on peut faire des analyses liées à la COVID-19 et aux plaintes liées aux escroqueries. On a tiré parti des canaux numériques y compris ceux plus traditionnels. Et comment est-ce que nous pouvons les lier avec des membres de la communauté, du grand public ? Est-ce que nous pouvons faire des campagnes de sensibilisation pour les encourager à mieux se protéger ou nous servir des canaux de plaintes ? Ces grands programmes de transferts sociaux sont créés pour atténuer les risques de fraude et autres pratiques abusives par des messages proactifs, des sondages à bénéfice, et cetera. Pour pouvoir intégrer les atténuations de risques de fraude et la protection du consommateur ; il y a un problème dans beaucoup de marchés où on trouve que les systèmes des gouvernements ne sont pas solides et la protection du consommateur du point de vue du fournisseur n'est pas solide. Nous avons vu un fournisseur sur le marché où le taux de résolution était d'environ 50 %, donc nous voulons améliorer ce chiffre. Avec les données nécessaires, nous pouvons surveiller ce domaine. C'est tout ce que j'ai à dire et merci d'avoir écouté.

>>BILEL JAMOUSSI : Merci beaucoup, Rafe Mazer de l'IPA d'avoir partagé au sujet de vos activités de l'IPA et comment tu travailles à étudier les escroqueries sur la COVID-19 sur les médias sociaux et le réseau mobile. En ce qui concerne aussi les actions avec les régulateurs que tu as recommandés à la fin de ta présentation. Mesdames et Messieurs, nous sommes arrivés à la fin des présentations et les participants peuvent continuer à soumettre les questions dans la foire aux questions en cliquant sur l'icône. Nous allons prendre les questions dans un petit moment. Nous aurons un petit dialogue avec les intervenants avec des questions en particulier.

À votre avis, quels sont les principaux défis auxquels sont confrontés les régulateurs dans le suivi des délits financiers numériques ? Quelqu'un veut y répondre ?

>>JAMI SOLLI : Oui. Un des plus grands défis c'est que les personnes ne veulent pas reconnaître qu'il y a un problème. Personne ne veut être reconnu comme capitale Ponzi dans le monde. La première étape est de regarder le niveau de dommage économique que ces escroqueries causent à tous les niveaux et de convaincre deuxièmement que les personnes devraient plus s'impliquer à ce sujet.

>>BILEL JAMOUSSI : Merci, Jami. Quelqu'un d'autre ?

>>RAFE MAZER : J'aimerais vite ajouter que dans certains marchés pouvoir avoir accès et communiquer avec les consommateurs est un défi important. Même si vous voulez les atteindre ils ne sont pas toujours conscients et sont susceptibles de ne pas avoir un bon téléphone ou de bonnes connexions dans des pays où ils n'ont même pas ce genre de facilité. C'est un grand défi qui rend le travail plus difficile dans certains pays.

>>BILEL JAMOUSSI : Merci.

>>ALEXANDER RESCH : Quand nous parlons des défis pour les régulateurs, c'est l'environnement actuel de paiement et l'environnement financier qui est très rapide et en évolution rapide. Il faut comprendre ce qui se passe dans le domaine financier des paiements numériques. Nous avons la limite du blanchiment d'argent et les régulateurs considèrent que c'est un défi de retracer et avec un développement rapide pour mettre en place les bonnes réglementations à ce sujet.

>>BILEL JAMOUSSI : Merci. Thomas ?

>>THOMAS SILKJAER : Je peux parler seulement des biens numériques. Mais les deux grands défis, c'est la multitude des différents genres de biens numérique rend presque impossible de surveiller le développement de l'espace. En ce qui concerne la connaissance et aussi le traçage et de travailler avec cela. Deuxièmement, les fournisseurs de biens numériques responsables qui s'impliquent dans nos activités. Dans mon travail, je rencontre les

fournisseurs de services qui vont au-delà de leurs exigences, qui font un excellent travail. Mais la plupart du temps il y a des fournisseurs de services qui font le minimum ou même pas. Il faut s'assurer que les fournisseurs de service sont responsables de leurs services. C'est très important.

>>BILEL JAMOUSSI : Assaf ?

>>ASSAF KLINGER : En ce qui concerne les escroqueries basées sur Internet, ce qui est le plus important, c'est lié au juridique. Il n'y a pas d'endroit pour les personnes où s'adresser. C'est un problème technologique qui est très difficile à comprendre. Il y a aussi un très grand problème de juridiction. Si j'ai une fraude en Afrique, mais l'argent de la fraude est envoyé en échange à Singapour, comment est-ce que le gouvernement, la police du Kenya fait face à la police de Singapour avec une fraude qui a fini chez toi, sur ton terrain ? En ce qui concerne Singapour c'est très facile parce que c'est un pays très développé, mais les échanges qui ont été mentionnés qui ne sont pas coopératif résident dans des endroits où la juridiction est assez faible et pour cette même raison c'est pour cela qu'ils réussissent. C'est le plus grand problème, à mon avis. C'est le besoin de la coordination au niveau mondial.

>>BILEL JAMOUSSI : C'est une très bonne continuation vers ma deuxième question : comment les partenariats public-privé et les organisations internationales comme l'UIT et INTERPOL peuvent fournir des orientations et des normes pour le suivi des crimes financiers numériques ?

>>ASSAF KLINGER : Ce que nous faisons à Fidji d'important c'est d'éduquer. Les gens ne sont même pas contents que cela se passe. La plupart des régulateurs n'ont aucune idée que cela se passe. Premièrement il faut éduquer le public et répandre la nouvelle et être bref. Après, il y aura plus d'idées.

>>BILEL JAMOUSSI : Merci.

>>ALEXANDER RESCH : Moi aussi j'aimerais répondre. Cela fait référence à ce qu'a dit Assaf. Du point de vue du maintien de l'ordre public, il y a beaucoup de choses qui sont rapportées sur le terrain et elles sont mises dans des ressources en ligne ou des sites en ligne de police, mais on peut en faire beaucoup plus à ce sujet. Par exemple, le complot Ponzi, cela pourrait être quelque chose qui pourrait faire l'objet d'une campagne de sensibilisation comme nous l'avons fait l'année dernière en octobre. Nous avons fait des campagnes Web qui ont eu beaucoup de succès. Cela pourrait être quelque chose qu'on pourrait faire avec l'UIT pour pouvoir accroître la sensibilisation à ce sujet. Parce qu'avec Internet et toutes les possibilités, il y aura toujours des personnes qui vont pouvoir faire des escroqueries.

>>BILEL JAMOUSSI : Oui, merci beaucoup. Quelqu'un d'autre ?

>>RAFE MAZER : Je vais répéter un peu ce que les autres ont dit jusqu'à présent ; la coordination des juridictions est extrêmement importante. J'ai vécu un cas au Kenya ; plusieurs personnes ont subi une escroquerie et les bitcoins ont été envoyés au Brésil et il n'y avait pas de juridiction pour que le Kenya puisse collaborer avec le Brésil. Cela se passe vraiment et les consommateurs sont laissés au milieu de complots internationaux.

>>JAMI SOLLI : Tous les intervenants ont très bien parlé pour se concentrer sur la prévention, mais le consommateur continue à investir pas dû au manque de connaissance à ce sujet, mais du point de vue de la pauvreté et par désespoir. Il y a des gens qui croient que quelque chose de bien va se passer et ils mettent leurs économies dans ces escroqueries et ils vont emprunter des fonds aussi. Il y a des effets intergénérationnels et dans l'escroquerie de l'Ouganda ils ont perdu toutes leurs économies de toute leur vie. La deuxième étape est la facilitation du crime qui se passe. Mon premier point, en ce qui concerne les consommateurs, les régulateurs ont du mal à communiquer leur message aux consommateurs en direct. Mais vous voyez l'exemple

du consommateur ; comment est-ce que le criminel s'y prend ? Les autres criminels vont s'imiter les uns et les autres, et cetera.

>>BILEL JAMOUSSI : Merci, Jami. Thomas ?

>>THOMAS SILKJAER : En ce qui concerne des partenariats entre le secteur public et privé, on parle d'une multitude de biens en ligne, ils ont différents réseaux qui se comportent de façon différente et ils ont des mécanismes de fraude différents. C'est difficile de créer un seul mode de surveillance de l'argent et de les appliquer à toutes les blockchains. En ce qui concerne le secteur public et les développements qui s'y passent, c'est très nécessaire de collaborer avec le secteur privé pour exiger des régulations et des analyses sur les blockchains.

>>BILEL JAMOUSSI : Merci. Pour résumer la première question, en ce qui concerne quels sont les défis clé pour les régulateurs pour faire face, pour conseiller les crimes financiers numériques et comment reconnaître le problème et son impact économique sur le grand public, éduquer les consommateurs, engager les régulateurs et reconnaître la multitude et la vitesse à laquelle la technologie travaille et pouvoir garder et l'importance de la juridiction internationale. Et comment maintenir le rythme, la cadence. Que pouvons-nous faire ? Accroître la sensibilisation, parler aux consommateurs de comment les escroqueries Ponzi ont commencé là et sont ciblées par les médias sociaux et d'autres canaux. Soyez conscients de la technologie en essor rapide et il faut parler au secteur privé qui a les outils pour pouvoir garder la cadence, maintenir la cadence avec cet essor rapide.

Maintenant, j'ouvre le micro. Je vois des questions des participants en ligne. Les intervenants peuvent voir les questions. Je commence par la première qui s'adresse à tout le monde, très bonne analyse, est-ce qu'il y a eu des efforts internationaux pour réguler la fraude qui est liée en partie au DLT ou est-ce que cela tombe dans le cadre établi ? Quels sont les avantages et les désavantages à celle sujet ? Quelqu'un

voudrait prendre la question d'Otari ?

>>JAMI SOLLI : Je n'ai pas vu que cela se passe comme cela, mais c'est peut-être une question pour une autre personne qui a fait des recherches sur la légalité de DLT.

>>BILEL JAMOUSSI : Merci, Jami. Je vais passer à la prochaine question. C'est une question qui s'adresse à Rafe et Jami ; quelle pression les régulateurs peuvent amener pour arrêter les mouvements SIM, le swapping ?

>>JAMI SOLLI : Certains pays comme le Kenya peuvent en parler, organiser des forums de fraude pour que les régulateurs rencontrent l'industrie pour parler des fraudes en cours. C'est un forum semi-privé où ils peuvent partager les informations directement avec les régulateurs et les régulateurs peuvent mettre de la pression pour passer à l'action peut-être.

>>BILEL JAMOUSSI : On peut passer à la prochaine question de Alex : comment les méthodes et les outils que nous avons à l'heure actuelle peuvent faire face à ces escroqueries financières structurelles comme la COVID-19 ?

>>ALEXANDER RESCH : Du point de vue de INTERPOL, nous voyons que les criminels tirent parti de la peur de la pandémie. Nous avons vu que ce genre d'équipement de protection personnel comme les masques et les kits de test de COVID-19 donne lieu à des escroqueries de livraison, de vente et ce sont aussi des biens contrefaits et qui tirent parti des fonds publics qui sont mis à la disposition du public pour la COVID-19. On voit que les criminels se débrouillent pour ouvrir des comptes bancaires ou blanchir l'argent par le biais du système bancaire en se servant de mules ou en établissant des entreprises fausses inscrites dans des circonstances spécifiques pour ouvrir des comptes bancaires et du point de vue de la banque, s'ils surveillent des activités anormales sur ces genres de comptes bancaires, il y a aussi des possibilités du point de vue des régulateurs qui doivent rapporter

ces institutions financières pour rapporter que ces activités louches se passent sur ces comptes bancaires, que quelqu'un reçoit tel et tel salaire mensuel et tout d'un coup ils ont reçu un tas de sous de la part d'une entité étrangère. Nous avons vu des exemples de ce genre. Qu'est-ce qui peut être fait à ce niveau.

>>BILEL JAMOUSSI : Thomas ? Est-ce que tu veux répondre ?

>>THOMAS SILKJAER : J'ai demandé un peu d'élaboration sur cette question de technologie financière.

>>BILEL JAMOUSSI : On passe à une autre question qui veut parler des escroqueries liées à la COVID-19 et aux équipements de protection personnelle et de soins de santé. En ce qui concerne les masques, est-ce que c'est la même chose dans les autres pays ? Est-ce que les escroqueries se servent de compte bancaire tiers ?

>>ALEXANDER RESCH : Les premières escroqueries ont commencé en Malaisie et les chaînes de fournitures, d'après ce que nous avons vu, les masques sont disponibles. Nous ne voyons pas beaucoup de victimes en Malaisie, mais nous voyons des victimes de ce genre dans les Amériques. Nous avons même vu des gouvernements, des ministères de la Santé qui sont victimes quand ils essaient d'acheter ce genre de masque, ils n'ont pas vraiment vérifié les sites depuis lesquels ils faisaient leurs achats. Du point de vue du blanchiment d'argent, une fois qu'un montant d'argent est transféré on essaie de l'intercepter, mais cela prend un ou deux jours pour que l'argent soit divisé dans des comptes en étages et on voit différent niveau et on voit que nous avons affaire à des cartels de blanchiment d'argent professionnel par lesquels c'est fait en quelques jours. Alors c'est très difficile pour le maintien de l'ordre public de poursuivre ce genre d'activité criminel.

>>BILEL JAMOUSSI : Une question de suivi de la même personne. En dépit des demandes officielles, les forces de l'autorité arrêtent ce genre de mouvement financier, est-ce que c'est possible d'avoir plus de points de contact ?

>>ALEXANDER RESCH : Désolé, mais je n'ai pas pu suivre toute la question...

>>BILEL JAMOUSSI : Même dans des demandes officielles, les pays sont susceptibles d'avoir de la difficulté pour poursuivre les cas et avoir les informations nécessaires.

>>ALEXANDER RESCH : Nous avons beaucoup de maintien de l'ordre public dans beaucoup de pays et nous assistons les cas qui émanent de la police. Nous avons un site public et nous proposons que les crimes soient rapportés aux agences nationales. S'il y a une victime de fraude d'investissement qui envoie un paiement en Royaume-Uni, on peut faire appel au Royaume-Uni. C'est eux qui s'occupent de l'enquête.

>>BILEL JAMOUSSI : Assaf, quels sont outil ?

>>ASSAF KLINGER : Je me sers d'outils qui se trouvent dans ma présentation aussi pour bitcoin. Pour Ethereum, on se sert d'un autre outil. Mais nous allons afficher un webinaire préenregistré ce qui sera bien plus long qui va traiter, qui va être un enseignement sur comment se servir de ces outils pour faire le repérage. Ce sera vraiment — nous allons afficher ce webinaire dans quelques semaines et ce sera bien plus détaillé.

>>BILEL JAMOUSSI : Une autre question sur les portefeuilles de cryptomonnaie qui ne sont pas toujours ouverts par des fournisseurs de services et qui sont susceptibles d'anonymat ; quelles sont les techniques d'enquête dans de telles circonstances ?

>>THOMAS SILKJAER : Il y a différents genres de compte sur Blockchain et les biens numériques. Il y a des comptes utilisés par les fournisseurs de services virtuels pour les paiements et toutes les opérations en admettant que le régulateur soit agréé au niveau officiel, c'est possible dans ce cas-là d'obtenir les informations concernant qui l'a envoyé ou reçu, et cetera. Mais tous les autres comptes bancaires sont en gros anonyme. Votre seul recours est de tracer le propriétaire d'un compte précis sur la base de l'historique des

opérations passées. Vous pouvez voir une relation avec un autre compte utilisé pour envoyer de l'argent en échange ou un fournisseur de services de cette façon-là vous pouvez déduire des relations ou des informations et c'est là où les algorithmes peuvent être utilisés pour identifier les groupes de transactions. Pour identifier ce genre de connexion et les identités derrière ces comptes anonymes.

>>BILEL JAMOUSSI : Merci. Jami? Une question sur ton succès pour faire face aux soins proactifs pour les clients ?

>>JAMI SOLLI : Il n'y en a pas beaucoup. On a réussi à recouvrer de grandes sommes d'argent ; pas 90 %, mais à peu près deux tiers de l'argent volé. En considérant les escroqueries, c'est mieux de se concentrer sur la prévention à l'avenir. C'est rare que les consommateurs vont recouvrer leur argent. Il y a eu un cas au Bangladesh et l'argent a été saisi, mais il n'y a pas une législation appropriée en place pour distribuer l'argent aux victimes. Cela s'est passé souvent. Les biens sont saisis, mais il n'y a pas distribution des fonds et les gouvernements n'essaient pas de redistribuer les fonds aux victimes.

>>BILEL JAMOUSSI : Est-ce qu'il y a un site où le grand public peut se diriger pour surveiller les portefeuilles suspects et les adresses suspectes, Alexander ?

>>ALEXANDER RESCH : C'est une très bonne idée et les collègues au niveau interne explorent les opportunités, mais c'est compliqué pour la disponibilité pour le grand public.

>>ASSAF KLINGER : Il y a beaucoup de sites communautaires à ce sujet, comme bitcoin et beaucoup d'autres. Je vais l'afficher sur la question même.

>>BILEL JAMOUSSI : Je crois que sur cela, on en vient à la fin de cet épisode. J'aimerais maintenant clôturer et remercier tous les intervenants de votre contribution et tous les participants de s'être joints à nous. J'ai vu que j'ai vu plus de 210 participants actifs à

un moment ou un autre dans notre webinaire d'aujourd'hui. Je vous invite au prochain épisode le 27 juillet où nous allons nous concentrer sur l'interopérabilité et la résilience de l'infrastructure des paiements numériques. J'aimerais remercier tout le monde de sa participation. Je vous souhaite à tous une très bonne journée ou une bonne soirée et je déclare ce webinaire clos. Merci à tout le monde et bon week-end.