Aidspan
Independent observer of the Global Fund

ENTRETIEN AVEC VIVIANA MANGIATERRA

Le site web « J'en parle, maintenant ! » (I Speak out Now »), le site web du Bureau de l'Inspecteur général offrant informations et ressources documentaires, présente de fréquentes mises à jour sur toutes les questions liées aux risques susceptibles d'intéresser les partenaires de mise en œuvre du Fonds mondial, allant de « Comment vous prémunir contre la fraude aux frais de scolarité » à « Lutter contre le hameçonnage », en passant par « Dénoncer les violations des droits humains ».

Dans un récent blog (en anglais), Katie Hodson, la Directrice des enquêtes du BIG, se concentre sur les « mutations de la fraude dans le monde » constatées dans les évaluations menées par le BIG sur la mise en œuvre des subventions du Fonds mondial. La veille permanente de ce « paysage » fait partie du rôle de madame Hodson afin de protéger les actifs et la réputation du Fonds mondial.
Ce qui sous-tend la thématique du blog de Hodson, et qui est également exprimé dans le rapport annuel 2018 du BIG, ce sont les données probantes et chiffrées qui montrent que la nature des cas de fraude les plus fréquents, commis dans le cadre de la mise en œuvre des subventions du Fonds mondial, a considérablement changé, passant d'une fraude principalement liée aux achats à une fraude liée à la formation, à la chaîne logistique et aux données des programmes. Il y a cinq ans, la plupart des allégations de fraude reçues par le BIG (11 cas en 2014-2015, soit 80% du total des cas) étaient liées aux achats. De nos jours, il y en a beaucoup moins (2 cas en 2018, soit 20%).

Selon Hodson, le mécanisme d'achats groupés du Fonds mondial est considéré comme un facteur positif ayant contribué à la réduction des cas de fraude liés aux achats, mais en contrepartie, cela signifie également que les fraudeurs invétérés recherchent désormais des domaines soumis à des contrôles moins stricts, comme par exemple certains éléments de la chaîne logistique nationale, tels que les entrepôts et les mécanismes de distribution mis en place par les gouvernements.

Le blog de Hodson traite des différents types de fraude (fraude aux achats, à la formation, aux indemnités journalières, détournement de fonds, falsification de données) et met en lumière les « nouveaux domaines de risque de fraude », qui sont également identifiés dans le rapport annuel 2018 du BIG, y compris la fraude aux données programmatiques (l'enquête du BIG de 2018 sur les données falsifiées en Guinée était la première de ce type) et les rétrocommissions sur salaire (lire l'article de l'OFM du 3 septembre 2018 – en anglais) .

À l'heure actuelle, les enquêtes du BIG sur la fraude se répartissent en quelques grandes catégories : 33% des enquêtes concernent des cas de fraude à la formation, 20% des cas liés à la chaîne logistique, 7% concernent des cas de détournement de fonds, 7% concernent des données manipulées, et 13% correspondent à d'autres combines tels que les rétrocommissions sur salaires et les cas de fraude aux frais de scolarité.

Alerter le BIG – les allégations de fraude

En 2018, le BIG a reçu 208 allégations de fraude (seulement une de plus qu'en 2017), dont 107 émanaient de « lanceurs d'alerte » et 35 provenaient directement du Secrétariat, ce que Hodson considère généralement comme « crédible », car les pistes émanant du Secrétariat proviennent souvent « des yeux et des oreilles de l'ALF [agent local du Fonds] sur le terrain ». (Le BIG a ouvert des enquêtes sur 64 de ces cas, soit 31%.)

« [Les ALF] sont ceux qui ont accès aux livres et aux registres », déclare Hodson. "Ce sont eux qui examinent les comptes. Les informations reçues [par le BIG] venant du Secrétariat ont donc souvent déjà été vérifiées."

Les lanceurs d'alerte restent cependant un maillon essentiel, affirme Hodson. « Nous encourageons toujours les gens à s'exprimer et à nous parler – mais l'alerte en temps réel est bien l'un des sujets qui m'empêchent de dormir », dit-elle, signifiant par là que parfois, les lanceurs d'alerte se manifestent bien longtemps après les malversations. "Lorsque le Secrétariat entend parler de quelque chose, nous souhaitons qu'il nous le dise dès que possible. [Et] nous encourageons les lanceurs d'alerte à tirer le signal d'alarme lorsqu'ils voient quelque chose qui semble inhabituel. "

De nouveaux types de fraude

Lors de son entretien avec l'OFM, Hodson s'est étendue sur le sujet des nouveaux types de fraude que le BIG constate de plus en plus de nos jours, notamment le problème relativement nouveau des données falsifiées (comme dans l'exemple de la Guinée en 2018) et des rétrocommissions sur salaire, sujets sur lesquels le BIG a actuellement trois nouvelles enquêtes en cours. Hodson a souligné que le cas de la Guinée avait provoqué une perte financière relativement faible (les dépenses non conformes s'élèvent à un total de $114 366), mais que cela avait conduit le BIG à adopter une approche de type « vitre brisée » dans ses enquêtes (où une infraction apparemment mineure peut signaler ou déclencher d'autres infractions plus graves).

Dans le cadre d'un nouveau cas de données falsifiées, qui fait actuellement l'objet d'une enquête du BIG, Hodson a déclaré que la fraude liée aux achats avait été identifiée en premier, et que cela avait conduit à une enquête plus approfondie. « Il est possible que là où, par le passé, le BIG se serait peut-être arrêté, nous nous sommes dit, vu qu'ils sont prêts à frauder sur les dépenses et les achats, quels autres services et activités mis en œuvre ont-ils pu falsifier ? Nous avons donc également tourné notre attention vers cela. »

Une autre méthode récente pour frauder implique un courriel de hameçonnage. Il s'agit d'un type d'attaque d'ingénierie sociale qui se produit lorsqu'un attaquant se fait passer pour une entité de

confiance et persuade une victime d'ouvrir un courrier électronique, puis de cliquer sur un lien malveillant. Ce lien peut conduire à l'installation de logiciels malveillants, révélant des informations sensibles ou des données importantes, que l'attaquant peut utiliser pour pénétrer un système ou un compte. (Source: www.imperva.com) Il s'agit du premier rapport signalant une attaque réussie de hameçonnage envers un bénéficiaire du Fonds mondial ayant entraîné une perte d'argent, a déclaré M. Hodson. Le rapport d'enquête du BIG sera publié dès que le BIG aura reçu une réponse du bénéficiaire à la « lettre de conclusion », que le BIG a déjà envoyée. Hodson n'était pas encore en mesure de rendre public le nom du pays ni les détails, mais les leçons tirées de ce cas seront partagées avec les autres bénéficiaires afin de les sensibiliser davantage aux risques.

« Nous savons grâce à nos collègues travaillant dans différentes organisations [internationales] que ce n'est pas la première fois que nos communautés de type ONG sont ciblées », a déclaré Hodson. « Il semble que ce soit une combine assez ciblée qui a également connu du succès dans d'autres organisations. » Le BIG développe à présent une ressource documentaire dans « J'en parle, maintenant ! » (qui viendra s'ajouter à sa collection de ressources et de documents d'E-apprentissage) pour informer les partenaires de mise en œuvre du Fonds mondial sur la façon de repérer les signaux d'alerte et de minimiser l'impact d'escroqueries similaires.

« C'est très bien de détecter ces combines », a déclaré Hodson à l'OFM, « mais nous voulons aussi nous assurer que nous limitons le risque que cela ne se reproduise, en investissant nos ressources dans des domaines qui peuvent réellement aider le Fonds mondial à atteindre son objectif. »

Un prochain article de l'OFM portera sur les enquêtes proactives du Bureau de l'Inspecteur général, ainsi que sur les enquêtes de supervision.

Read More