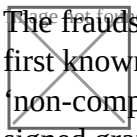
OIG INVESTIGATION OF PHISHING FRAUD IN SENEGAL FINDS “MULTIPLE CONTROL LAPSES” WITHIN MINISTRY OF HEALTH AND SOCIAL ACTION

In an investigation of Global Fund grants to Senegal, the Office of the Inspector General (OIG) found that Global Fund monies destined for the purchase of tuberculosis diagnostic equipment, for Senegal’s Tuberculosis/Resilient and Sustainable Systems for Health grant, were unwittingly transferred to fraudsters posing as the Principal Recipient’s (PR) supplier.



The fraudsters hacked the email account of a PR procurement specialist via a phishing email. This is the first known fraud of this kind within a Global Fund grant. The OIG has classified the misdirected funds as ‘non-compliant expenditures,’ given that the payment made was not in line with payment provisions in the signed grant agreement.

The OIG’s investigation report was made public on 4 November 2019.

There was no suggestion in the report that the Principal Recipient, Senegal’s Ministry of Health and Social Action (MHSA) or the PR’s procurement specialist colluded in the fraud. However, the OIG report said, “insufficient vigilance, controls, and reporting at MHSA,” especially the controls regarding changes to beneficiaries’ bank account details, allowed the fraud to succeed.

The OIG reported the fraud to the national police in the unnamed Eastern European country. (The OIG explained to the GFO that for reasons related to preventing a similar type of fraud from happening again, they preferred not to give details about the fraud scheme or its country of origin.) The national police reported that the bank account to which the fake payment had been made was empty, the funds having been redirected to several different bank accounts within that country. The procurement agent, a United

Nations-based organization, has requested via its internal audit entity that the UN Office of Legal Affairs refer the case to national authorities (at the time of publication there was no further information about the nature of these "national authorities," ie. which national body the referral was transmitted to).

What happened: the chain of events leading to the fraud

The fraud began in early August 2018, after the email account of a procurement specialist at Senegal's Ministry of Health and Social Action (MHSA) was hacked following a phishing email sent on 6 August. (Individuals posing as supplier staff began exchanging emails with the procurement specialist; this gave them an entry point to hack the email account.) The fraudsters were then able to see and control messages sent and received by the procurement specialist's email account. They also used at least five fake supplier email addresses, the OIG found, to make the Procurement Specialist believe that he/she was receiving emails from staff at the genuine supplier (the fraudsters used a foreign fake mailer to send the fake emails; there was no security breach to the genuine supplier's email accounts or IT systems.)

The fraudsters (whose identity is still not known) tapped into a procurement-in-process for tuberculosis diagnostic equipment, consisting of GeneXpert testing machines and microscopes. On 31 August 2018, the fraudsters, posing as known staff from the genuine supplier, instructed the procurement specialist to make payment for the equipment purchase to a bank account in an Eastern European country instead of to the New York-based JP Morgan account specified in the project agreement signed with the UN-based procurement agent. MHSA's finance division then instructed their bank to transfer the $481,541 for the diagnostic equipment to the new account.

Impact and immediate actions taken

The Agreed Management Actions (AMAs; see 'Main findings' section below) recommended by the OIG are designed to address the controls-related weaknesses the OIG has identified in the PR's international procurement-related activities.

However, a number of immediate actions have been taken in addition to address the main control issues highlighted by this review: the MHSA has created server-based email accounts for its staff; the Global Fund has stopped all PRs from paying the supplier of GeneXpert machines and microscopes directly (only payments directly from the Global Fund to the supplier are allowed); the project agreement between the PR and the supplier is now available in French; and the Local Fund Agent is temporarily tasked with reviewing, before payment, all PR payments above a certain threshold.

Origins of the OIG investigation

The fraud came to light because the procurement specialist, having received no reply to several emails he/she had sent to follow up on the order after payment, sent a further email that copied an employee from the genuine supplier.

In November 2018, both the supplier and the MHSA reported the fraud to the Global Fund Secretariat, who then alerted the OIG to the wrongdoing. For this investigation, an OIG team conducted an in-country mission to Senegal. The team interviewed several PR staff members, the genuine supplier, and analysed data from the procurement specialist's computer as well as his/her smartphones and email accounts.

Main findings and Agreed Management Actions (AMAs)

Below we summarize the report's two main findings and their associated AMAs:

2.1 $481,541 of grant funds were unwittingly transferred to fraudsters posing as the PR's supplier

This finding unpacks the main events relevant to the fraud: that email hacking of the Procurement Specialist's Yahoo account was at the origin of the fraud (allowing the fraudsters to assume the email identities of the supplier's staff, and to obtain a copy of the approved quote of $427,244 for GeneXpert machines and $54,297 for microscopes); that

payment was authorized to an Eastern European bank account, and that there was no evidence of collusion between the Procurement Specialist and the fraudsters.

AMA 1: The Secretariat will finalize and pursue an appropriate recoverable amount. (Due by 31 October 2020, owned by the Chair of the Recoveries Committee.)

AMA 2: The Secretariat will ensure that the PR provides an action plan to ensure the security of its IT systems used to manage Global Fund grants, and to raise awareness among staff and sub-recipients about this fraud, as well as how to report a case of hacking. (Due by 31 March 2020, owned by the Head of Grant Management.)

2.2. Multiple control lapses at the Ministry of Health and Social Action combined to allow the fraud to succeed

The OIG concluded that this phishing fraud was only possible due to a series of control lapses within the MHSA, and that if any one of these lapses had been corrected, that might have prevented the wrongdoing from occurring. (See pages 7-8 of the report for further detail.)

The lapses were: The 'phishing' attack itself (via a Yahoo email account used for personal and professional purposes), the lack of controls related to changing MHSA beneficiaries' bank account details, the Procurement Specialist's lack of vigilance, the lack of timely notification of the hacking (the Procurement Specialist became aware that his/her Yahoo account had been hacked on 3 October but did not inform his/her supervisors), and the lack of a French-language project agreement between the PR and the supplier (the French-speaking Procurement Specialist confirmed to the OIG that he/she could not understand the English-language project agreement, which is believed to have contributed to the lack of vigilance regarding the request to change bank account details), and a lack of cyber-security training for staff in sensitive roles.

AMA 3: The Secretariat will ensure that the PR formalizes its manual of procedures, and its procedures on how to process international procurements, including specific control responsibilities. (Due 31 March 2020, owned by Head of Grant Management.)

AMA 4: The Secretariat will send a letter to all Global Fund PRs drawing their attention to this report's findings, and recommending the formalization of their guidelines on procedures and controls to perform before changing a supplier's bank details. (Due 31 March 2020, owned by Head of Grant Management.)

(See the full table of AMAs on page 9 of the OIG report.)

Senegal context

The Global Fund has committed a total of $350 million to Senegal, and has disbursed a total of $332 million. Senegal currently has four active Global Fund grants: two for HIV, one for malaria, and the TB/RSSH one affected by this phishing fraud, called 'Improving the health of the Senegalese population and implementing the End TB strategy in Senegal'.

Table 1: Senegal's currently active Global Fund grants

Active Grant	Grant	Grant component	S
SEN-Z-MOH	Ministry of Health and Social Action of the Republic of Senegal	TB/RSSH	
SEN-H-ANCS	Alliance Nationale des Communautés pour la Santé	HIV	
SEN-H-CNLS	Conseil National de Lutte contre le SIDA de la République du Sénégal	HIV	
SEN-M-PNLP	Ministry of Health and Social Action of the Republic of Senegal	Malaria	

Source: Data obtained from

Further reading:

- The investigation report: ‘Global Fund Grants in Senegal: Internet phishing fraud resulting in loss of $481,541 of grant funds’ is accessible on the Global Fund website
- An article from GFO 361 (31 July 2019), ‘OIG Head of Investigations describes ‘changing fraud landscape’ in Global Fund grants’.

Read More