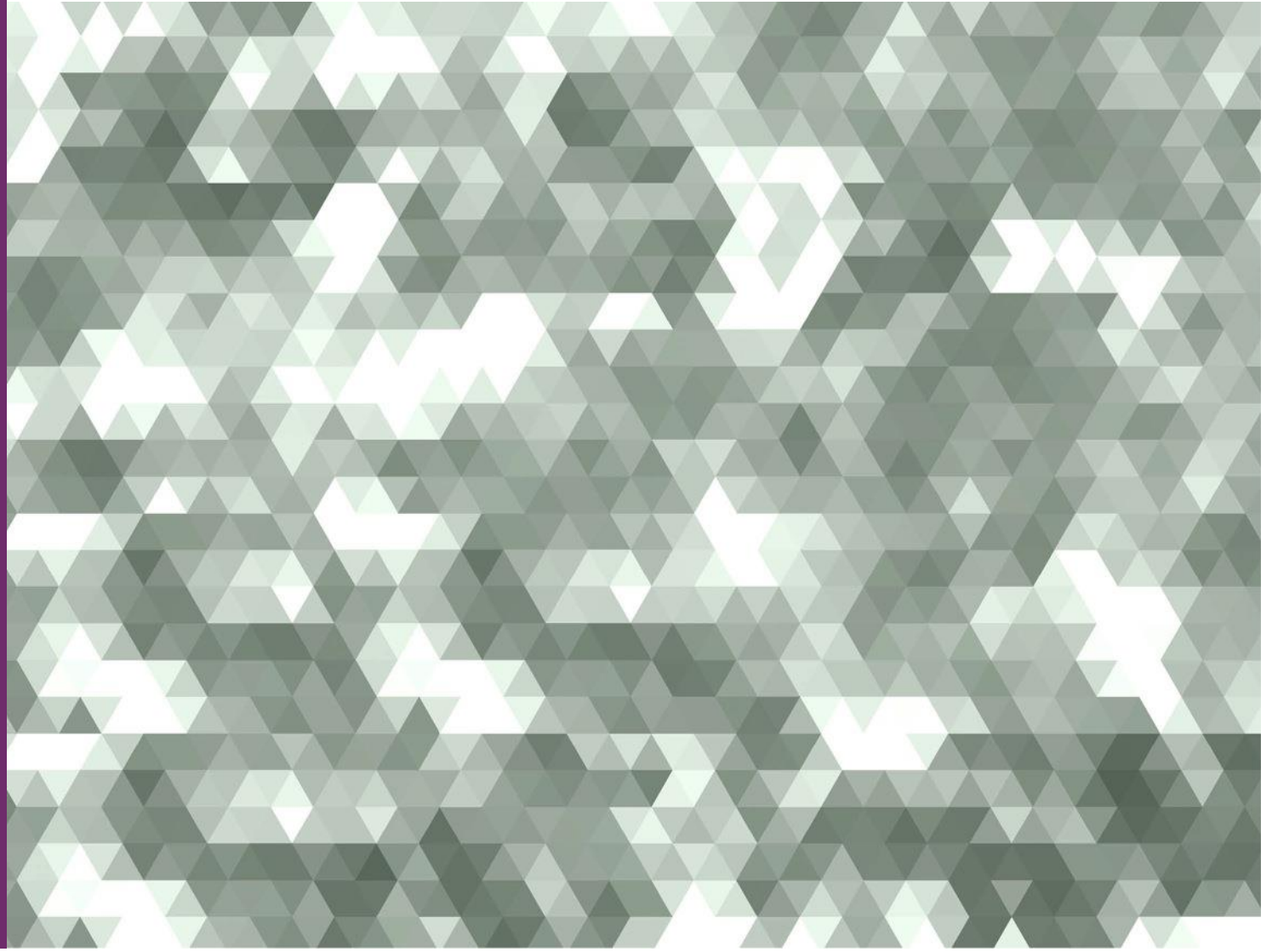

Investigation Report

Global Fund Grants in Senegal

Internet phishing fraud resulting in loss of US$481,541 of grant funds

GF-OIG-19-020
4 November 2019
Geneva, Switzerland

The Global Fund
Office of the Inspector General

What is the Office of the Inspector General?

The Global Fund has zero tolerance for fraud, corruption and waste that prevent resources from reaching the people who need them. Through its audits, investigations and advisory work, the Office of the Inspector General safeguards the Global Fund's assets, investments, reputation and sustainability, reporting fully and transparently on abuse.

If you suspect irregularities or wrongdoing in programs financed by the Global Fund, you should report them to the OIG.

Online Form >
Available in English, French, Russian, Spanish
Email: hotline@theglobalfund.org
Free Telephone: +1 704 541 6918

Learn about fraud, abuse and human rights violations at the OIG's e-learning site, **www.ispeakoutnow.org**

Table of Contents

1. Investigation at a glance 3
1.1. Executive summary 3
1.2. Genesis and scope 3
1.3. Findings 3
1.4. Impact 4
1.5. Context 4
2. Findings 5
2.1. US$481,541 of grant funds were unwittingly transferred to fraudsters posing as Global Fund suppliers 5
2.2. Multiple control lapses at the Ministry of Health and Social Action combined to allow the fraud to succeed 7
3. Table of Agreed Management Actions 9
Annex A: Schedule of key events 10
Annex B: Methodology 11

1. Investigation at a glance

1.1. Executive summary

In August 2018, individuals posing as supplier staff began exchanging emails with the Procurement Specialist at Senegal's Ministry of Health and Social Action (MHSA), the Principal Recipient (PR) for the Global Fund's Tuberculosis/RSSH grant in the country, regarding the purchase of tuberculosis diagnostic equipment.

The Procurement Specialist's personal email account, which was also used for professional purposes, had been hacked, allowing fraudsters to control messages sent and received by the Procurement Specialist's account. The fraudsters assumed the identities of supplier staff already known to the MHSA staff member.

On 31 August 2018, the fraudsters instructed the Procurement Specialist to make payment for the equipment not to the supplier's bank account referred to in the project agreement signed with the procurement agent, but to a different account in Eastern Europe unconnected to the supplier. MHSA's Division of Finance Administration and Staff subsequently instructed their bank to transfer US$481,541 to this new account. The fraud came to light afterwards, when the Procurement Specialist copied a genuine supplier employee in an email to the fraudsters.

Insufficient vigilance, controls and reporting at MHSA, most notably controls related to changing beneficiaries' bank account details, allowed the fraud to succeed.

Non-compliant expenditures: ***US$481,541***

Proposed recoverable amount: ***US$481,541***

Start of wrongdoing: ***August 2018***

OIG alerted to wrongdoing: ***November 2018***

Source of alert: ***Supplier and PR through Global Fund Secretariat***

1.2. Genesis and scope

In November 2018, both the supplier and the Principal Recipient reported the fraud to the Global Fund Secretariat, who then alerted the OIG. They reported that a Procurement Specialist at the Ministry of Health and Social Action had been duped into requesting the PR's Division of Finance Administration and Staff to transfer funds designed for the procurement of GeneXpert testing machines and microscopes to a third-party bank account in Eastern Europe.

An OIG team investigated the fraud and conducted an in-country mission to Senegal. Investigators performed an in-depth analysis of data from the Procurement Specialist's computer, smartphones and e-mail accounts, and interviewed several PR staff members and the supplier.

1.3. Findings

The investigation confirmed that US$481,541 of grant funds were unwittingly transferred to unknown owners of a bank account in Eastern Europe.

An unknown third party hacked and took control of the Procurement Specialist's mailbox, through a phishing email. The unknown fraudster(s) then duped the PR's Procurement Specialist into requesting MHSA accounting department to transfer grant funds to a bank account in Eastern Europe, without arousing suspicion.

The investigation did not find any evidence of collusion between the PR's Procurement Specialist and the fraudsters. Nevertheless, multiple control lapses at MHSA contributed to the ease with which the fraud was able to occur.

1.4. Impact

The investigation exposed several control lapses in Global Fund-related international procurements managed by the Principal Recipient. These weaknesses will be addressed through Agreed Management Actions.

The OIG concludes that US$481,541, the total amount of grant funds that were disbursed to a third-party bank account as a result of the fraud, are non-compliant expenditures, as the disbursement was not in line with the provisions of the signed grant agreement. The Global Fund Secretariat, at its discretion, may request the Principal Recipient to reimburse this non-compliant expenditure.

To address the key control issues identified during the investigation, the following immediate actions have been taken:

- MHSA created server-based mailboxes for its staff members.
- The Global Fund has stopped all PRs from paying the supplier of GeneXpert machines and microscopes directly. Only payments from the Global Fund to the supplier are allowed. This requirement will be included as a provision in Global Fund budgeting guidelines for the next funding cycle.
- The Project Agreement signed by MHSA and the procurement agent has been translated into French, to be understandable by all staff involved in concerned procurements.
- Temporarily, the Local Fund Agent is reviewing all Principal Recipient payments above a certain threshold, prior to payment.

1.5. Context

Every year, approximately 10 million people fall ill with tuberculosis (TB) worldwide, but only six million are identified. GeneXpert machines (pictured on the right) use sophisticated molecular technology to test if a person is infected with tuberculosis, and if so, whether the TB bacterium is resistant to common TB drugs. GeneXpert machines are more accurate and yield much faster results than traditional TB diagnosis methods. Each machine can run 16 tests per day, i.e. over 5,000 patients per year. The machines are also used for HIV testing and thus their availability and use play a significant role in the Global Fund's fight against tuberculosis and HIV.

In Senegal, the World Health Organization estimates that there are 14,000 new tuberculosis cases and 3,000 deaths from TB each year. The GeneXpert machines and microscopes which MHSA planned to purchase were meant to be deployed in six priority regions, including Dakar, the capital city, where half of tuberculosis cases are concentrated.

The Global Fund has invested over EUR 23 million in the fight against tuberculosis in Senegal since 2003, and currently has one TB/RSSH active grant in the country.

Table 1. Active TB/RSSH grant

Active grant	Principal Recipient	Grant Components	Signed amount (EUR)
SEN-Z-MOH	Ministry of Health and Social Action	Tuberculosis/ Resilient and Sustainable Systems for Health (RSSH)	10,743,845

2. Findings

2.1. US$481,541 of grant funds were unwittingly transferred to fraudsters posing as the Principal Recipient's supplier

A Procurement Specialist at the Direction of Equipment and General Administration (DAGE), part of the Ministry of Health and Social Action of Senegal, was tricked by unknown fraudsters posing as MHSA suppliers into requesting the transfer, which was subsequently authorized by DAGE management, of US$481,541 of grant funds to a third-party bank account in Eastern Europe. The payment was due prior to the delivery of equipment.

A schedule of key events relevant to the above is set out in Annex A.

Email hacking at the origin of the fraud

The fraudsters hacked into the Procurement Specialist's Yahoo account and, assuming the identities of MHSA supplier staff known to the Procurement Specialist, exchanged several emails with the MHSA employee from a fake mailer, relating to the planned purchase of GeneXpert machines and microscopes for the respective amounts of US$427,244 and US$54,297.

The fraudsters sent the Procurement Specialist a countersigned copy of the approved quote for the equipment, drawing the Procurement Specialist's attention to the fact that the supplier's bank account details had changed. The signed quote contained details for an account in Eastern Europe unknown to the Procurement Specialist and unconnected to the procurement agent.

Payment was authorized to an Eastern European bank account

Subsequently, MHSA Division of Finance Administration and Staff, on behalf of the Head of DAGE, instructed MHSA's bank, Crédit du Sénégal, to authorize the two payments to the fraudulent bank account.

Following the transfer, the Procurement Specialist sent several emails to the fraudsters, asking when the equipment would be delivered; all of these went unanswered. On 15 November, while sending another reminder, the Procurement Specialist copied a genuine staff member at the supplier, thus alerting them to the exchange.

The supplier wrote to the Procurement Specialist and to the Global Fund Country Team, explaining that they had not received any previous emails, had not requested a change in bank account details, and had not received payment for the equipment. A week later the Head of DAGE wrote to the Global Fund's Fund Portfolio Manager (FPM) for Senegal, explaining what had happened. The Global Fund Country Team notified OIG about the fraud.

Subsequently, OIG reported the fraud to national police in the Eastern European country, who advised that the bank account to which the money had been transferred was now empty, the funds having been redirected to several different bank accounts in the country.

The procurement agent is a United Nations-based organization in charge of administering the supplier's financial resources. The procurement agent's Internal Audit and Investigation Group has requested the UN Office of Legal Affairs to refer the case to national authorities for legal recourse.

No evidence of collusion between the Procurement Specialist and the fraudsters

The OIG found no evidence which indicates that the Procurement Specialist colluded with the fraudsters to perpetrate the fraud, that the Procurement Specialist knew the fraudsters or had been in touch with them before August 2018, or was aware that a fraud was being perpetrated.

Agreed Management Action 1

☑ Based on the findings of the report, the Global Fund Secretariat will finalize and pursue, from all entities responsible, an appropriate recoverable amount. This amount will be determined by the Secretariat in accordance with its evaluation of applicable legal rights and obligations and associated determination of recoverability.

Owner: Chair, Recoveries Committee

Due date: 31 October 2020

Agreed Management Action 2

☑ Based on the findings of the report, the Global Fund Secretariat will ensure that the Principal Recipient, Ministry of Health and Social Action, provides an action plan to ensure security of all its IT systems used for management of Global Fund's grants, and to raise awareness of its staff and Sub-recipients about the fraud scheme applied in that case and the reporting process in case of hacking.

Owner: Head, Grant Management Division

Due date: 31 March 2020

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

The fraud detailed in this investigation was only possible due to a series of control lapses within the Ministry of Health and Social Action, any one of which, if corrected, might have thwarted the wrongdoing.

The Procurement Specialist was subjected to a 'phishing' attack

'Phishing' emails are sent by fraudsters masquerading as known, trustworthy individuals or entities; they lure members of the public to reveal sensitive information such as usernames, passwords, credit card or bank account details. In many cases, the user's computer is infected, allowing the fraudsters to take control of the target's email account and to send further phishing emails from it. Via forensic analysis, the OIG found that a phishing email sent on 6 August 2018, was the likely source of the Procurement Specialist's email account being hacked.

After hacking the account, the fraudsters used at least five fake supplier email addresses to make the Procurement Specialist believe he/she was receiving emails from a genuine supplier staff member. The fraudsters used a foreign fake mailer to send the fake emails. The supplier confirmed to the OIG that there had been no security breach to its IT systems.

Lack of controls related to changing beneficiaries' bank account details

The Ministry of Health and Social Action's manual of procedures for Global Fund-related operation does not specify controls to be performed by procurement and accounting departments in case of a requested change in a supplier's bank account. Typical controls to reduce the risk of fraud in changing supplier's bank account could include formal procedures around the maintenance of supplier's bank account details, independent validation of all requested changes in suppliers' bank accounts, and adequate segregation of duties in the processing of payments. In this case, neither the Procurement Specialist nor the three other DAGE staff involved in the procurement validation conducted any controls beyond comparing the bank account reported on the pro-formas with the bank account details provided by the fraudsters.

Lack of vigilance of the Procurement Specialist

DAGE's Head of Procurement Monitoring and Planning, and the Director of DAGE, were both involved in the procurement's validation; they were however both new to the organization and this was their first Global Fund-related direct procurement. The Procurement Specialist did not flag to either individual the singular request for a change in bank account, which precluded them from questioning and challenging the change request. The Procurement Specialist notified only the accountant in charge of executing Global Fund-related payments about the change of bank account.

Lack of timely notification of the hacking

The Procurement Specialist became aware that his/her Yahoo account had been hacked on 3 October 2018, after contacts alerted him/her that they were receiving suspicious emails from that account. The Procurement Specialist did not however inform his/her direct supervisor (the Head of Procurement Monitoring and Planning), or the Director of DAGE, that his/her Yahoo account had been hacked, despite the account being used for both professional and personal purposes. The lack of timely reporting of the hacking is likely to have prevented the Procurement Specialist's supervisors and other concerned stakeholders from taking prompt action in the period immediately following the transfer to the fraudulent bank account, at which point it may still have been possible to prevent it.

Lack of a French-language project agreement between the Principal Recipient and the Supplier.

The Project Agreement signed between the Ministry and the procurement agent specifies that all procurement payments shall be paid to a JP Morgan bank account in New York. At the time the Procurement Specialist processed the procurement of TB diagnosis equipment, that project agreement was only available in English, however. The Procurement Specialist, a French-speaker, confirmed to the OIG that he/she could not understand the content of the project agreement. The fact that the Procurement Specialist and other staff involved in the validation process did not understand the content of the project agreement is likely to have contributed to the lack of vigilance regarding the request for the change of bank account submitted by the fraudsters.

Lack of cyber-security training for staff in sensitive roles

None of the DAGE staff in sensitive roles, such as those managing payments and procurements, have received any cyber-security training, increasing their vulnerability to hacking, notably of cloud-based mailboxes.

Since the fraud occurred, MHSA has created server-based (as opposed to cloud-based systems such as Yahoo) mailboxes for all staff, and instructed staff working on Global Fund-related grants to use them for their communications. However, the OIG found that as of March 2019, some staff continue to use their cloud-based mailboxes for business purposes.

Agreed Management Action 3

☑ Based on the findings of the report, the Global Fund Secretariat will ensure that the Principal Recipient, Ministry of Health and Social Action, formalizes in its manual of procedures, procedures on how to process international procurements, specifying control responsibilities of each stakeholder, if applicable.

Owner: Head, Grant Management Division

Due date: 31 March 2020

Agreed Management Action 4

☑ The Global Fund Secretariat will issue a notice letter to all Global Fund Principal Recipients drawing their attention to the findings of this report and recommending them to formalize in their internal manual of procedures guidelines on controls to perform before changing supplier's bank account, which include a direct confirmation from concerned suppliers for all payments above a relevant threshold determined in accordance with the Global Fund Secretariat.

Owner: Head, Grant Management Division

Due date: 31 March 2020

3. Table of Agreed Management Actions

Agreed Management Action	**Target date**
1. Based on the findings of the report, the Global Fund Secretariat will finalize and pursue, from all entities responsible, an appropriate recoverable amount. This amount will be determined by the Secretariat in accordance with its evaluation of applicable legal rights and obligations and associated determination of recoverability. *Owner: Chair, Recoveries Committee*	31 October 2020
2. Based on the findings of the report, the Global Fund Secretariat will ensure that the Principal Recipient, Ministry of Health and Social Action, provides an action plan to ensure security of all its IT systems used for management of Global Fund's grants, and to raise awareness of its staff and Sub-recipients about the fraud scheme applied in that case and the reporting process in case of hacking. *Owner: Head of Grant Management Division*	31 March 2020
3. Based on the findings of the report, the Global Fund Secretariat will ensure that the Principal Recipient, Ministry of Health and Social Action, formalizes in its manual of procedures, procedures on how to process international procurements, specifying control responsibilities of each stakeholder, if applicable. *Owners: Head, Grant Management Division*	31 March 2020
4. The Global Fund Secretariat will issue a notice letter to all Global Fund Principal Recipients drawing their attention to the findings of this report and recommending them to formalize in their internal manual of procedures guidelines on controls to perform before changing supplier's bank account, which include a direct confirmation from concerned suppliers for all payments above a relevant threshold determined in accordance with the Global Fund Secretariat. *Owner: Head, Grant Management Division*	31 March 2020

Annex A: Schedule of key events

Date	Event
6 Aug 2018	A phishing email is sent to the Procurement Specialist's Yahoo account; this is likely the source of the hacking. With access to the Procurement Specialist's Yahoo account, the fraudsters could monitor and manipulate his/her emails.
16 Aug 2018	The Procurement Specialist sends to the supplier approved quotes for the procurement of TB diagnostic equipment.
21 Aug 2018	The Procurement Specialist receives an email from a fraudster using a fake supplier email address, asking him/her when payment for the diagnosis equipment will be made.
31 Aug 2018	The fraudsters send the Procurement Specialist a quote for the diagnostic equipment on stamped, letterheaded paper of the supplier, including the fraudulent bank account details.
17 Sep 2018	The Head of Administration and Finance, on behalf of the Direction of Equipment and General Administration, instructs the Ministry's bank to authorize payment of US$481,541 to the bank account in Eastern Europe.
3 Oct 2018	The Procurement Specialist realizes that his/her Yahoo email account has been hacked but does not inform his/her supervisors.
31 Oct 2018	The Procurement Specialist emails the fraudsters asking for an update regarding the equipment's delivery. No response is received.
5 & 12 Nov 2018	The Procurement Specialist sends further reminder emails to the fraudsters, which also go unanswered.
15 Nov 2018	The Procurement Specialist, in writing to the fraudsters, copies a bona fide supplier staff email address, alerting them to the correspondence. The supplier staff member replies, explaining they were unaware of the previous email exchanges. The Procurement Specialist forwards the fraudulent equipment transfer order to the supplier.
16 Nov 2018	The supplier replies to say that the bank account details used for the transfer were wrong and unconnected to the supplier.
19 Nov 2018	The supplier reports to the Procurement Specialist and the Global Fund that the funds were not received, and the email addresses used were fake.
27 Nov 2018	The Head of the Direction of Equipment and General Administration explains the fraud to the Global Fund's Fund Portfolio Manager.

Annex B: Methodology

Why we investigate: Wrongdoing, in all its forms, is a threat to the Global Fund's mission to end the AIDS, tuberculosis and malaria epidemics. It corrodes public health systems and facilitates human rights abuses, ultimately stunting the quality and quantity of interventions needed to save lives. It diverts funds, medicines and other resources away from countries and communities in need. It limits the Global Fund's impact and reduces the trust that is essential to the Global Fund's multi-stakeholder partnership model.

What we investigate: The OIG is mandated to investigate any use of Global Fund funds, whether by the Global Fund Secretariat, grant recipients, or their suppliers. OIG investigations identify instances of wrongdoing, such as fraud, corruption and other types of non-compliance with grant agreements. The Global Fund Policy to Combat Fraud and Corruption[1] outlines all prohibited practices, which will result in investigations.

OIG investigations aim to:

(i) identify the nature and extent of wrongdoing affecting Global Fund grants;
(ii) identify the entities responsible for such wrongdoing;
(iii) determine the amount of grant funds that may have been compromised by wrongdoing; and
(iv) place the Global Fund in the best position to recover funds, and take remedial and preventive action, by identifying where and how the misused funds have been spent.

The OIG conducts administrative, not criminal, investigations. It is recipients' responsibility to demonstrate that their use of grant funds complies with grant agreements. OIG findings are based on facts and related analysis, which may include drawing reasonable inferences. Findings are established by a preponderance of evidence. All available information, inculpatory or exculpatory, is considered by the OIG.[2] As an administrative body, the OIG has no law enforcement powers. It cannot issue subpoenas or initiate criminal prosecutions. As a result, its ability to obtain information is limited to the access rights it has under the contracts the Global Fund enters into with its recipients, and on the willingness of witnesses and other interested parties to voluntarily provide information.

The OIG bases its investigations on the contractual commitments undertaken by recipients and suppliers. Principal Recipients are contractually liable to the Global Fund for the use of all grant funds, including those disbursed to Sub-recipients and paid to suppliers. The Global Fund's Code of Conduct for Suppliers[3] and Code of Conduct for Recipients provide additional principles, which recipients and suppliers must respect. The Global Fund Guidelines for Grant Budgeting define compliant expenditures as those that have been incurred in compliance with the terms of the relevant grant agreement (or have otherwise been pre-approved in writing by the Global Fund) and have been validated by the Global Fund Secretariat and/or its assurance providers based on documentary evidence.

Who we investigate: The OIG investigates Principal Recipients and Sub-recipients, Country Coordinating Mechanisms and Local Fund Agents, as well as suppliers and service providers.

[1] (16.11.2017) Available at https://www.theglobalfund.org/media/6960/core_combatfraudcorruption_policy_en.pdf
[2] These principles comply with the Uniform Guidelines for Investigations, Conference of International Investigators, 06.2009; available at: http://www.conf-int-investigators.org/?page_id=13, accessed 1.12.2017.
[3] Global Fund Code of Conduct for Suppliers (15.12.2009), § 17-18, available at: https://www.theglobalfund.org/media/3275/corporate_codeofconductforsuppliers_policy_en.pdf, and the Code of Conduct for Recipients of Global Fund Resources (16.07.2012), §1.1 and 2.3, available at: https://www.theglobalfund.org/media/6011/corporate_codeofconductforrecipients_policy_en.pdf. Note: Grants are typically subject to either the Global Fund's Standard Terms and Conditions of the Program Grant Agreement, or to the Grant Regulations (2014), which incorporate the Code of Conduct for Recipients and mandate use of the Code of Conduct for Suppliers. Terms may vary however in certain grant agreements.

Secretariat activities linked to the use of funds are also within the scope of the OIG's work.[4] While the OIG does not typically have a direct relationship with the Secretariat's or recipients' suppliers, its investigations[5] encompass their activities regarding the provision of goods and services. To fulfill its mandate, the OIG needs the full cooperation of these suppliers to access documents and officials.[6]

Sanctions when prohibited practices are identified: When an investigation identifies prohibited practices, the Global Fund has the right to seek the refund of grant funds compromised by the related contractual breach. The OIG has a fact-finding role and does not determine how the Global Fund will enforce its rights. Nor does it make judicial decisions or issue sanctions.[7] The Secretariat determines what management actions to take or contractual remedies to seek in response to the investigation findings.

However, the investigation will quantify the extent of any non-compliant expenditures, including amounts the OIG proposes as recoverable. This proposed figure is based on:

(i) amounts paid for which there is no reasonable assurance that goods or services were delivered (unsupported expenses, fraudulent expenses, or otherwise irregular expenses without assurance of delivery);
(ii) amounts paid over and above comparable market prices for such goods or services; or
(iii) amounts incurred outside of the scope of the grant, for goods or services not included in the approved work plans and budgets or for expenditures in excess of approved budgets.

How the Global Fund prevents recurrence of wrongdoing: Following an investigation, the OIG and the Secretariat agree on management actions that will mitigate the risks that prohibited practices pose to the Global Fund and its recipients' activities. The OIG may make referrals to national authorities for criminal prosecutions or other violations of national laws and support such authorities as necessary throughout the process, as appropriate.

[4] Charter of the Office of the Inspector General (16.05.2019), § 2, 10.5, 10.6, 10.7 and 10.9 available at: https://www.theglobalfund.org/media/3026/oig_officeofinspectorgeneral_charter_en.pdf
[5] Charter of the Office of the Inspector General § 2, and 18.
[6] Global Fund Code of Conduct for Suppliers, § 16-19.
[7] Charter of the Office of the Inspector General § 9.1.