PFSCM
Partnership for Supply Chain Management

+1-571-227-8600
pfscm@pfscm.org
www.pfscm.org

2733 Crystal Drive, 4th Floor
Arlington, VA 22202
USA

PFSCM Policy Document

Fraud and Corruption reporting

1. Purpose

To establish our commitment to global standards and practices, articulate those practices that are prohibited, and link these to our commitment to PFSCM's Integrated Anti-Corruption and Fraud Prevention Framework.

2. Background

PFSCM is built on a foundation of strong ethical practices and remains committed to applying the standards outlined herein consistently in all of its work. PFSCM is committed to an environment where open, honest communications are the expectation, not the exception. PFSCM wants to ensure that all its staff members feel comfortable in approaching their supervisor or designated personnel in instances whenever one believes violations of PFSCM policies and corresponding SOPs or WIs have taken place, in addition to utilizing the reporting mechanisms below.

This Policy[1] aims to capture international best practices from the following main sources: The Global Fund's Policies & Procedures, The United Nations Global Compact Principles,[2] and the United States Government's regulatory framework.

In addition, PFSCM daily work is to abide (when applicable) by the regulations cited below (please note that this does not intend to be exhaustive, but a general listing of reference):

- The UN Global Compact Principles
- The Global Fund's Policies on Procurement and Supply Management of Health Products
- The Global Fund's Procurement Policy
- The Global Fund's Policy Manual
- The Global Fund's Policy to Combat Fraud and Corruption
- The Global Fund's Ethics and Integrity Framework
- The Global Fund's Code of Conduct for Suppliers
- The Global Fund's Whistle-Blowing Policy and Procedures
- The Global Fund's Office of Inspector General reports on best practices on fraud reporting

- The Global Fund's Insurance Guidelines for Global Fund Grants
- The Global Fund's My Code, My Responsibility, whenever applicable
- The provisions of the corresponding to any Outsourced Services Agreement as part of any associated Pooled Procurement Mechanisms, and all applicable Global Fund and host country rules and regulations
- USAID's Automated Directive System (ADS) 303 Grants and Cooperative Agreements
- USAID's Automated Directive System (ADS) 302 Direct Contracting
- 2 CFR 200, Uniform Administrative Requirements, Cost Principles and Audits Requirements (e.g., 2 CFR 200.336, 2 CFR 200.331; 2 CFR 200.207; 2 CFR 200.113, Subpart F, etc.)[3]
- 2 CFR Subpart C – Post Award Requirements. (e.g., 215.21 Standards for financial management systems)
- 2 CFR 700, USAID Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards
- AIDAR 752.225-70, Source and Nationality
- 22 CFR Part 228 Source and Nationality[4]
- ADS 310, Source and Nationality Requirements for Procurement of Commodities and Services Financed by USAID
- ADS 591, Financial Audits of USAID Contractors, Recipients, & Host Government Entities
- ADS 206, Prohibition of Assistance to Drug Traffickers
- ADS 636, Project Funded Advances
- ADS 312, Eligibility of Commodities
- 2 CFR 180, OMB Guidelines to Agencies on Government-wide Debarment & Suspension
- 22 CFR 216, Environmental Procedures
- 31 USC 6301-6308, Federal Grant and Cooperative Agreement Act
- 48 CFR, Federal Code of Regulations (e.g., FAR 52.203-13: Reporting Requirements; FAR 52.222-50: Anti-Human Trafficking);
- The provisions of the corresponding project task order, contract and/or cooperative agreement, and all applicable USG and host country rules and regulations.

The Fraud Awareness, Anti-Corruption Policy, and Business Ethics Code & Compliance Framework can be defined as the body of internal policies, procedures, and controls that regulate PFSCM's daily work and interactions with any third party, which is reflected in its SOPs, New Employee Trainings, and different Codes of Conduct. All new staff members must review and acknowledge mandatory policies and SOPs and comply with any trainings as applicable on: Code of Conduct, Business Ethics, Respectful Workplace, Ethics in Research and Publication, among others.

3. Policy Statement

This policy applies to all PFSCM's funded activities, directly or indirectly, through all of its contractual mechanisms (included, but not limited to, partners, counterparts, subcontractors, stakeholders, and beneficiaries), in whole or in part, through its programs or any other form of payment, regardless of location of payment(s).

This Policy covers the following institutions and individuals (hereinafter, 'covered parties'):

a. Governance Level: PFSCM Board Members, Senior Management, focal points, members of any committee, internal technical review panel, or any other advisory or parent (or affiliated) entity of the PFSCM.

b. PFSCM Staff Members: In addition to Senior Management members, this also includes seconded staff, contractors, and interns, regardless of length of affiliation or the organization that they are employed by, or affiliated with.

c. Counterparties: Regardless of contractual arrangements (e.g., IQCs, IDIQs, Task Orders, Subcontracts, Sub agreements, Grants Under Contract, Consultant agreements, etc.) or type of contract relationship (e.g., governmental, commercial, or otherwise: including, without limitation, vendors, consultants, whether individuals or entities, local fund agents, and any other providers of goods and services), including their respective directors, officers, employees, affiliates, agents, of the foregoing.

PFSCM has a zero-tolerance approach towards Prohibited Practices, and details adequate responses inCode of Business Conduct and Ethics and Whistleblower policies. Responses could include disciplinary actions, recovery of funds, termination of contractual arrangements, referrals to supranational and/or national administrative, civil or criminal activities, conditional continued engagement, and/or other compensatory or punitive damages as may be available and applicable.

Alignment with International, National Anti-Fraud and Anti-Corruption Norms

PFSCM has aligned its internal Terms and Conditions - with existing best practices, including pledging to the UN Global Compact's Ten Principles, in particular Principal 10: "Business should work against corruption in all its forms, including extortion and bribery."

PFSCM will engage with its partners in the collective effort to raise awareness, prevention, detection, & response to fraud & corruption and reaffirms its commitment to transparency in all of its activities, and the essential role accountability plays in every funded program.

Funding Agencies Own Anti-Corruption Requirements

PFSCM recognizes that its SOPs, WIs, and internal control systems must be compliant with its funding agencies' requirements, policies, and procedures. PFSCM manages its risks in a consistent and practical manner as established in PolicyRisk Management, which identifies the different types of risks and opportunities applicable to PFSCM. This facilitates proactively identifying risks or opportunities, likelihood of occurring, consequence(s) if encountered, and mitigation plans on all of its divisions . Fraud risk exposure is assessed periodically by PFSCM to identify specific potential schemes and events that PFSCM needs to mitigate.

PFSCM has established a dual reporting process in line with its most important sources of funding that are of best practice nature aimed at avoid and/or mitigate potential key fraud risk and – if applicable – a corrective action plan.

Types of Payment Fraud: In addition to those Fraudulent & Prohibited Practices below, PFSCM is also incorporating "Payment Fraud," which can be considered any type of false or illegal transaction completed by a cybercriminal:

a) Phishing[5]: Phishing/Spoofing: Both terms deal with forged or faked electronic documents. Spoofing generally refers to the dissemination of email, which is forged to appear as though someone other than the actual source sent it. Phishing also referred to as vishing, smishing, or pharming, is often used in conjunction with a spoofed email. It is the act of sending an email falsely claiming to be an established legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specific website. The website, however, was set up only as an attempt to steal the user's information and is not genuine.

b) Identity theft: Identity theft exists outside of the digital realm as well, but it is a common type of fraud online. A cybercriminal who steals personal information and uses it under false pretense is engaging in identity theft. Hackers penetrate firewalls through old security systems or by hijacking login credentials via public Wi-Fi.

c) Pagejacking: Hackers can reroute traffic from your e-commerce site by hijacking part of it and directing visitors to a different website. The unwanted site may contain potentially malicious material that hackers use to infiltrate a network security system.

d) Advanced fee and wire transfer scams: Hackers target credit card users and e-commerce store owners by asking for money in advance in return for a credit card or money at a later date.

e) Merchant identity fraud: This method involves criminals setting up a merchant account on behalf of a seemingly legitimate business and charging stolen credit cards. The hackers then vanish before the cardholders discover the fraudulent payments and reverse the transactions.

When this happens, the payment facilitator is liable for the loss and any additional fees associated with credit card chargebacks.

f) Business Email Compromise (BEC):[6] A sophisticated scam targeting businesses working with foreign suppliers and companies that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

g) Data Breach:[7] A leak or spill of data, which is released from a secure location to an untrusted environment. Data breaches can occur at the personal and corporate levels and involve sensitive, protected, or confidential information that is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.

Additional Prohibited Practices: PFSCM's Prohibited Practices are those explicitly stated as such in its own Code of Business Conduct & Ethics, Whistleblower Policy, and all applicable SOPs & corresponding WIs. This policy attempts to complement the already existing Prohibited Activities:

a) Coercive Practices: Impairing or harming, or threatening to impair or harm, directly or indirectly, any party or the property of the party to improperly influence the actions of a party. For avoidance of doubt, this includes without limitation reputational or other impairment or harm, as well as physical harm.

b) Collusive Practices: An arrangement between two or more parties designed to achieve an improper purpose, including influencing improperly the actions of another party. For avoidance of doubt, this includes without limitation arrangements involving PFSCM's staff members and/or third parties that are intended to, or may have the effect of or result in, circumvention of PFSCM policies, regulations, or procedures.

c) Money Laundering: (i) the conversion or transfer of property, directly or indirectly, knowing that such property is derived from criminal activity, or helping any person who is involved in such activities evade the legal consequences of their actions, (ii) concealing or disguising the illicit origin, source, location, disposition, movement, or ownership of property knowing that such property is derived from criminal activity, or (iii) the acquisition, possession, or use of property, knowing at time of receipt that such property is derived from criminal activity.

d) Obstructive Practices: (i) deliberately destroying, falsifying, altering, or concealing evidence material to an inquiry by PFSCM, or making false statements in order to materially impede a PFSCM inquiry into allegations of Prohibited Practices, (ii) threatening, harassing, or intimidating any party to prevent it from disclosing, or as retaliation for disclosing, its knowledge of matters relevant to a PFSCM inquiry or from pursuing the inquiry, (iii) engaging in acts that impede the exercise of PFSCM's access rights, including the access rights described in this Policy, or (iv) failing to comply with the duty to report as defined in the Whistleblowing Policy in a timely manner.

Duty to Report

In addition to the compliance with the aforementioned regulations, PFSCM staff members are expected to report violations, per below:

a. Parallel Reporting: There are multiple channels by which PFSCM may become aware of allegations of fraud (e.g., Incident Management, Ethicspoint, Senior Management conversations) and reports these as required to funding agencies' particular requirements and as per decision by Senior Management, in conjunction with Contracts and HR.

Resources for reporting for some of PFSCM key clients are as follows:

A. Funding Agency (e.g., USAID or TGF). Via the designated Point of Contact representative (i.e., Contracts and/or Technical Lead), and/or to the Funding Agency Fraud Reporting Hotline, fraud violations will be reported.

1. As part of the Transparency and Accountability Internal Controls, PFSCM also provides all available resources that the USG tools offer, e.g., Office of Inspector General, Contractor Self-Disclosure FAQ: https://oig.hhs.gov/faqs/contractor-faq.asp which contains guidance on how to disclose "in writing situations for which they have credible evidence of a potential violation of the civil False Claims Act or Federal criminal law involving fraud, conflict of interest, bribery, or gratuity."

2. The Global Fund's Office of the Inspector General available online resources, including versions in different languages: https://www.theglobalfund.org/en/oig/#related-resources.

3. TGF's "I Speak Out Now!" initiative, which is designed to encourage grant implementers to denounce fraud, abuse, and human rights violations in the programs financed by TGF: http://www.ispeakoutnow.org/

b. EthicsPoint™: As a subsidiary of JSI R&T, PFSCM covered parties or others (including at a country level) must file an anonymous, confidential report of the alleged violation at 7 days a week, 24 hours a day. Anyone can use the Code of Conduct Helpline, hosted by third party hotline provider NAVEX/EthicsPoint, to make a report, raise an issue, or simply ask questions.

c. PFSCM Incident Management System: PFSCM staff are required to report all PFSCM-related non-conformance or potential non-conformance incidents through its internal incident management system d. Mandatory Disclosures: This particular section is applicable only for those activities funded by the USG provided that they are also incorporated into the award mechanisms in the following fashion: In case of USG-funded programs, (e.g., grants, cooperative agreements) and should there be an inclusion of 2 CFR 200.113: The non-Federal entity or applicant for a Federal award must disclose, in a timely manner, in writing to the Federal awarding agency or pass-through entity all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. ADS 303 STANDARD CLAUSE M28: Consistent with 2 CFR §200.113, applicants and recipients must disclose, in a timely manner, in writing to the USAID Office of the Inspector General, with a copy to the

cognizant Agreement Officer, all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Subrecipients must do the same and additionally disclose this information to the prime recipient. Recipients must include this mandatory disclosure requirement in all subawards and contracts. For other contractual arrangements (e.g., acquisition, i.e., contracts), the requirements are set forth in FAR 52.203-13, Contractor Code of Business Ethics and Conduct, i.e., timely disclosure, in writing, to the agency OIG, with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of any Government contract performed by the Contractor or a subcontractor thereunder, the Contractor has credible evidence that a principal, staff member, agent, or subcontractor of the Contractor has committed a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 U.S.C. or a violation of the civil False Claims Act (31 U.S.C. 3729- 3733).

e. Any subsequent assessment and the rationale for taking the decision to investigate / not investigate must always be fully recorded.

f. Involving OIG:[8] PFSCM considers that 'fraud is fraud' regardless of amounts involved. Whenever evidence is credible, PFSCM turns it over to OIG. In GF-funded programs, it is recommended that isolated[9] instances of fraud perpetrated by an individual, resulting in minor losses, can and must be dealt with by PFSCM, without the immediate involvement of the respective OIG, except when the lost amounts could be material or when the issue is identified as potentially systemic, involving one or more individuals over time, then the OIG should be alerted immediately (if in doubt, consult Contracts or Chief Operating and Financial Officer). PFSCM is to provide the respective OIG (and its Focal Point) with copies of internal investigation reports relating to the funding agency resources as well as any recommended remedial actions to mitigate risk of similar future occurrence.

Protection Against Retaliation: PFSCM implements and maintains processes to prevent, detect, and respond to any retaliation against any Covered Person who, consistent with PFSCM's Ethical Framework and the Whistleblowing Policy, reports any of the Prohibited Activities including in all applicable SOPs and WIs, as well as this Policy. In summary, it is the responsibility of all individuals to report in good faith any concerns they may have regarding actual or suspected activities, which may be illegal or in violation of PFSCM's policies, and PFSCM strictly prohibits any demotion, harassment, or any other form of retaliation against individuals who report suspected violations in good faith.

Communications with Donors, External Auditors, and Government Authorities: When communicating to donors or external parties about allegations or inquiries, staff members may reach out to the Chief Operating and Financial Officer prior to submitting. The goal is to ensure that PFSCM does not provide donors with hearsay or conjecture(s), which may prove later to be inaccurate or unrelated to their funding.

PFSCM Fraud Awareness, Anti-Corruption Policy, and Business Ethics Code and Compliance Framework: In addition to the above-stated, this Framework also attempts to be consistent with international & national best practices, by the following means:

a. Example and Tone at the Senior & Management Levels.

b. Fraud and Corruption Risk Assessment

c. Policies & Procedures (e.g., Code of Conduct, COI, Risk Management, Due Diligence)

d. Training & Communication

e. Whistleblowing and Investigations

f. Response: enforcement, sanctions, and other remedies

g. Reporting & Testing of Internal Control Systems

h. Reporting to Board

For additional reference, PFSCM may also use USG reports, such as: USAID Practitioner's Guide for Anti Corruption Programming, USAID Anti Corruption Assessment Handbook, TGF Office of Inspector General: Thematic Review of Fraud Reporting, TGF My Country, My Responsibility, and, FBI: Internet Crime Annual Reports. These reports are a great resource for providing guidance on best practices for 'key conditions' for anti corruption effectiveness, remaining vigilant against cyberattacks and scams and reporting them immediately to the project implementing leadership by identification of varying patterns of corruption, and programming responses to administrative corruption.

Periodic Reviews and Incorporation of Best Practices: All successful awareness and compliance plans must be subject to periodic reviews of the ethics and compliance programs or measures, designed to evaluate and improve their effectiveness in preventing and detecting foreign bribery, taking into account relevant developments in the field, and evolving international and industry standards.

PFSCM Accountability for Overseeing and Implementing this Policy

Senior Management has ultimate ownership over this policy to embody the highest standards of integrity against fraud and corruption. Senior Management delegates the oversight of matters relating to the Policy and its implementation as follows:

- Director
- CO/FO
- Contracts Manager
- HR Manager

[1] This Policy is modeled as per the Global Fund's Policy to Combat Fraud & Corruption.

[2] PFSCM is a signatory member of "The Ten Principles of the UN Global Compact."

[3] Please check the resources found at: www.ignet.gov for Single Audit Guides, under "Manual & Guides" section.

[4] Please keep in mind the $250,000 or less threshold and the authorized geographic code for procurement of all goods and services. Standard Provisions for U.S. Nongovernmental Organizations, a Mandatory Reference for ADS Chapter 303.

[5] https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud

[6] FBI: https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud

[7] Id as above

[8] Office of the Inspector General refers to the Global Fund's & USAID's respective reporting entity.

[9] OIG Report. Thematic Review of Fraud Reporting. Recommendations. July 2017. PFSCM attempts to incorporate the best practices and recommendations in this policy