

ANTI-FRAUD AND WHISTLE BLOWER POLICY

1 General Statement

The fraud and whistle-blower policy for British Gold Trust (BGT) is established to outline the controls in place to educate, prevent, detect, and report any form of fraudulent behavior.

By definition, “Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.” BGB Board and Senior Management have a strong commitment to fraud risk management. This document serves to convey the expectations of the Board of Directors and Senior Management. Examples of fraud can include but are not limited to these three categories.

1.1 Financial Misstatement

- Forgery or alteration of any financial document;
- Improper revenue recognition;
- Misappropriation of funds, securities, supplies, or other assets
- Understatement of liabilities;
- Management Override;
- Deviation from full and fair reporting of the financial condition.
- Misappropriation of Assets
- Misappropriation of funds, supplies, or other asset;
- Impropriety in the handling or reporting of money or financial transactions;
- Use of BGB-owned assets for personal use;
- Loss or misuse of BGB resources by not following system controls.

1.2 Misconduct

- Theft of a payment or other financial asset;
- Profiting as a result of insider knowledge;
- Impropriety in the handling or reporting of money or financial Transactions
- Confidential information used in the conduct of outside business;
- Disclosing information that should be secure;
- Noncompliance with internal controls.

1.3 Staff Awareness

Each employee shall have a basic understanding of fraud and be aware of the red flags and know their role within the internal control framework. Fraud involves not just monetary issues, but also is significant to an organization’s financial reporting, operations, reputation, legal, and regulatory compliance. Staff has an awareness of how their job procedures are designed to help mitigate fraud risks and when noncompliance may open up the opportunity for fraud to occur. Each member of the management team

will be familiar with the types of improprieties that might occur within their area of responsibility and will be alert for any indication of possible irregularity.

1.4 Fraud Red Flags and Mitigation Options

Frequent “red flags” indicating fraud opportunities include:

- Poorly written or poorly enforced internal controls, procedures, policies or security;
- Irregular or unexplained variances in financial reporting;
- Failure to take action on audit findings;
- Unusually high expenses or purchases;
- Frequent complaints from customers;
- Missing or incomplete files, records, and documentation;
- Employee comments concerning possible fraud;
- Complex business arrangements not widely understood and appear to serve little or no purpose;
- Financial results that seem “too good to be true”;
- A consistently close match between reported results and planned results;
- Changes to employee’s behavior.

Prior to employment, background checks are used in employment screening with the specific objective of assuring that persons with inappropriate records or inconsistency are identified and eliminated from the hiring process. Every employee is required to read and understand policies and procedures upon employment with BGB.

Ongoing monitoring procedures are built into normal recurring operating activities. Certifications and self-assessments create strong controls that help prevent occurrences of fraud. Segregation of duties exists and is tested routinely. The annual fraud risk assessment, which is a part of annual BGB risk assessment process, helps to identify potential schemes and events.

Other internal controls help prevent fraud as follows:

- Adherence to documentation and authorization limits;
- Physical security and restricted access;
- Independent review;
- Clear lines of authority;
- Enforcement of conflict of interest;
- Internal control walkthroughs;
- Regular vacation breaks;
- Board oversight;
- Anonymous Reporting “Whistle-blower” Procedures.

These controls help to create an environment where employees, vendors, and other parties believe that dishonest acts will be detected, reported, and dealt with appropriately.

2 Reporting and Complaint Procedures

Employees, vendors or other parties with concerns of fraud or suspected fraud may report directly to the Chief Risk officer (CRO). The information below lists information

for the current CRO. Any fraud that is detected or suspected must be reported immediately.

CRO upon receipt of a complaint, CRO will take appropriate action for investigation, tracking and confidentiality.

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to GFS. It is important to provide as much information regarding the facts and circumstances surrounding the complaint as possible in order to facilitate a full and complete investigation.

Upon receipt of a complaint, CRO will determine whether the complaint actually pertains to accounting or auditing matters and, as possible, acknowledge receipt of the complaint to the sender. Complaints relating to accounting or auditing matters will be forwarded for investigation to such person or persons as CRO determines to be appropriate. Confidentiality will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review.

GFS is committed to achieving compliance with all applicable securities laws, regulations, accounting standards, accounting controls, and audit practices.

Any employee, vendor, or other party may file a good faith complaint without the fear of dismissal or retaliation of any kind. GFS will not discharge, demote, suspend, threaten, harass or in any manner discriminate against anyone because of any lawful actions in providing information or other assistance in investigation of fraud or the commission

This will be true even in the event that it is concluded from the investigation that no violation occurred.

This policy will be reviewed and approved by the GFS Board annually.