MUTUAL TRUST LIFE INSURANCE COMPANY,

A Pan-American Life Insurance Group Stock Company

ANTI-FRAUD HANDBOOK

2021 Update

This Anti-Fraud Handbook is presented in the following sections:

I. PREAMBLE

Mutual Trust Life Insurance Company, a Pan-American Life Insurance Group Stock Company (hereinafter collectively referred to as "the Company" or "Mutual Trust") (NAIC #66427), maintains high standards and is committed to protecting its insureds' private information. The Company's Anti-Fraud Plan (the "Plan") outlines the Company's commitment to creating an anti-fraud community, and maintaining high ethical standards in its administration of insurance policies.

This Plan is designed to prevent, detect and deter fraud and to take effective action against any attempted or actual fraudulent act affecting the Company. This Plan makes it clear to all concerned that appropriate and decisive action will be taken against those committing or attempting to commit fraudulent acts against this Company. In order for the Company to be effective in its approach to dealing with the problem of fraud it has to set into place and create a community of intolerance rather than indifference to such matters.

What constitutes *Fraud*?

"Fraud" generally involves an act of intentional deception, bribery, forgery, extortion, theft, misappropriation, false representation, conspiracy, corruption, collusion, embezzlement, or concealment of material facts. Fraud may be committed by an individual, a group of individuals, or by one or more organizations. It may be committed to benefit an individual (such as theft of time or falsification of expense records) or to benefit the Company (such as misstatement of revenue). Fraud is a violation of trust that, in general, refers to an intentional act committed to secure personal or business advantage.

Fraud includes offenses such as theft, corruption, false accounting, forgery, counterfeiting and blackmail. In the insurance context, fraud may not necessarily involve an employee of the company. Many insurance companies are the victims of fraud through the submission of false or misleading statements by a policyholder, agent or provider in support of an insurance application or claim.

II. PLAN STRATEGY

We expect all of our employees, insureds and agents to be fair and honest and provide all the assistance and support needed to deal with fraud should it occur. They should abide by established rules, procedures, codes and recommended practices.

This Plan outlines the elements of the Company's Systematic Anti-Fraud Strategy needed to discourage fraud through the organization. This Strategy addresses the procedures for preventing, detecting, investigating and reporting fraud which, despite best practices, can occur. The Plan also addresses the company's training program. The elements of the Company's Systematic Anti-Fraud Strategy are as follows:

A. The establishment of a Special Investigative Unit;
B. Fraud Education & Training;
C. Fraud Detection Procedures;
D. Fraud Investigation Procedures;
E. Recovery/Litigation/Prosecution related to Fraud;
F. Cooperation and Access;
G. Fraud reporting to government authorities and law enforcement; and
H. T he maintenance of an anonymous hotline for the reporting of fraud by employees, customers and Vendors.

Anti-Fraud Coordinator

The Anti-Fraud Coordinator, who is also the Deputy General Counsel and Compliance Officer for Mutual Trust, is responsible for the continued maintenance of this anti-fraud plan and oversight of the processes governing the prevention and detection of Home Office fraud and the coordination of any investigation of suspected frauds, both internal and external, among the responsible business units. All irregularities detected or suspected must be reported to the Anti-Fraud Coordinator or his/her designee so that documented and approved actions will be taken, including contacting law enforcement and any other required government agencies when appropriate.

The Anti-Fraud Coordinator has the primary responsibility for coordinating the investigation of Home Office and external fraud allegations at the Company. While investigations will generally be conducted in-house, depending on the nature of the allegations, the Anti-Fraud Coordinator may choose to engage the assistance of outside legal counsel, outside Special Investigations Unit (SIU) and/or appropriate law enforcement authorities. If any outside firm is utilized, steps will be taken to assure that such firms meet all applicable jurisdictional licensing requirements.

If the investigation reveals that fraudulent activities have occurred, the Anti-Fraud Coordinator or his/her designee will notify the General Counsel, independent Special Investigations Unit, proper executives, legal counsel and, if appropriate, the Company's Board of Directors.

The Anti-Fraud Coordinator or independent Special Investigations Unit will also notify the appropriate law or regulatory enforcement body, in writing if required, that a fraud has occurred.

The Anti-Fraud Coordinator is responsible for receiving relevant information on a confidential basis from an employee, policyholder, insured, General Agent, writing agent, or third party who suspects dishonest or fraudulent activity. The individual providing information should contact the Anti-Fraud Coordinator and should not attempt to personally conduct investigations or interviews related to suspected fraud (see Reporting Procedures Section VII).

The results of investigations conducted by the Anti-Fraud Coordinator, independent Special Investigations Unit, or designee will not be disclosed or discussed with anyone other than those persons who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected (but subsequently found innocent) of wrongful conduct, to protect confidential sources of information and to protect the Company from potential civil liability.

Deputy General Counsel

A part of the responsibilities attributable to the Deputy General Counsel is the reviewing and monitoring of sales and marketing materials and activities. In addition, the Deputy General Counsel is responsible for overseeing the handling and response to formal policyholder and client complaints. All General Agents and their Agents are responsible for prompt notification of policyholder and client complaints to the Deputy General Counsel.

General Counsel

The General Counsel has full responsibility for all legal matters affecting the Company.

III. PREVENTION & DETERRENCE

The Company recognizes that fraud is costly, both in terms of reputational risk and financial losses. The prevention of fraud is therefore a key objective for the Company's Special Investigative Unit (herein after known as SIU).

The Company recognizes that Company Employees are often the first line of defense in preventing fraud. A key preventative measure in that fight is the effectiveness of its employees. Financial regulations place responsibility for fraud prevention on all employees. Every employee should be alert and report to their supervisor any suspicion of a fraudulent act and/or the possibility of fraudulent acts.

The Company requires its employees to act honestly, with integrity and to safeguard any Company resources for which they are responsible at all times. Each employee is governed in their work by the Company's Corporate Code of Conduct Policy as well as various other policies and procedures administered throughout the Company. Employees are expected to always be aware of the possibility that fraud and/or theft may exist in the workplace.

Deterrence: There are a number of ways to deter individuals from committing or attempting to commit fraudulent acts, whether they are inside or outside of the Company:

Use of Fraud Warnings: All of the Company's applications for insurance and claim forms should have a fraud warning that states in substance: "Any person who knowingly, and with intent to injure, defraud, or deceive an insurance company, files a statement of claim containing any false, incomplete, or misleading information is guilty of insurance fraud, which is a felony." This language may vary in order to comply for specific state requirements as shown in Appendix 4.

Additional Deterrence Tools:

a) Company's publication of its commitment to fight against fraud and reinforces this at every opportunity (i.e. The Company website and Intranet site, clauses in contracts, statements of benefits forms, publications, etc.);

b) Corporate actions that are strong and decisive when fraud is suspected and proven (i.e. termination of contracts, prosecution, etc.); and

c) Sound internal controls systems that minimize the opportunity for fraud and identify potential patterns of fraud.

General Agents and Writing Agents

The Company recognizes that General Agents and Writing Agents are independent business persons representing insureds and potential insureds, and are not employees of the Company. However, the Company expects all independent agents to abide by and cooperate with the Company's Anti-Fraud plan. The Company has put systems in place to monitor the actions of General Agents and Writing Agents and will take appropriate steps as warranted.

All General Agents, their agents and employees are the Company's partners in the prevention and detection of insurance fraud and other irregularities. All General Agents, their agents and employees are responsible for compliance with applicable insurance laws and regulations. General Agents must maintain procedures that would reasonably deter such wrongful acts. General Agents, their agents, and employees should be familiar with the types of improprieties that might occur within his/her area of responsibility and be alert for any indication of irregularities.

All irregularities detected or suspected by General Agents, their agents, and employees must be reported to the Company's Anti-Fraud Coordinator. Any investigative activity required will be conducted without regard to the suspected wrongdoer's relationship with the Company.

Senior management reviews all new Agent appointments. The application process includes a background check that may include inquiries to state insurance regulators. The Company also verifies that the Agent has the appropriate licenses and qualifications in the necessary state(s). The Agent must follow the hiring

policies and procedures provided by the Company. The *Guide to Business Practices* outlines the policies and procedures and should be referred to.

Agents are encouraged to visit the Mutual Trust agent website to review this Anti-Fraud Handbook, as well as the *Guide to Business Practices*. Agents are expected to develop an understanding of the Company's products and services and are required to sign the approved Ethics Statement, acknowledging receipt and understanding of the document. Each General Agent has the responsibility to supervise his/her agents and employees according to the guidelines set forth by the Company, and they are required to communicate the Anti-Fraud policy and Ethics Statement to them.

Policyholders, Insureds, Clients and Beneficiaries

All policyholders, insureds, clients and members of the general public have a responsibility for preventing and detecting insurance fraud and other irregularities. The management of the Company encourages policyholders, insureds, clients, beneficiaries and others to act in a lawful and proper manner and to report all allegations of insurance fraud or irregularities to the Company.

Home Office Policies and Procedures

The Company has adopted numerous Corporate Policies intended for the early detection of fraudulent activity. The Corporate Policies that address fraud include the Company's: i) Customer Identification Process; ii) Industry endorsed Underwriting Guidelines; iii) Suitability policy which includes its commitment to only process business which is suitable for the customer's needs and attempts to identify fraudulent transactions along with stranger owned life insurance arrangements; iv) Replacement Procedures utilized to assure that all replacements are justified; v) Complaint Procedures which attempt to identify the root cause of complaints including the commission of potential fraudulent activity; vi) Complaint Log which tracks agent complaints, inquiries, and trends, vii) Red Flag Policy which is designed to identify identity theft and other fraudulent behavior; and viii) Agent and Employee Disciplinary Procedures for the commission of fraudulent acts which include the potential for termination. The Company recognizes that fraud deterrence is a continual process, and in order to make the Company less vulnerable to fraud, additional procedures will be considered and implemented as deemed necessary.

Monitoring Reviews

The Company maintains internal Monitoring Procedures to remain assured that all adopted procedures implemented to identify fraud are functioning as designed. Among the Monitoring Procedures adopted are Quarterly Replacement Data Reviews, Semi-Annual Suitability Reviews, an Annual Complaint Data Review, along with strict compliance to a Monthly Monitoring Schedule established to review all procedures relied upon to enforce this Anti-Fraud Policy.

In addition, periodically an independent review and assessment of the anti-fraud program is conducted. The purpose of this review is to:

A) Provide an independent, objective business risk assessment of the policies and procedures in place at the Company targeted at the prevention, deterrence and early detection of fraud and related wrongful acts;
B) Assess the awareness level of the existing anti-fraud program and plan in all departments;
C) Determine whether the overall anti-fraud program in place remains accurate, relevant and effective; and
D) Assure compliance with all regulatory and legal requirements.

The Company maintains records of how it evaluates the effectiveness of its anti-fraud plan and retains these records for the future review of State Insurance Administrators.

Anti-Money Laundering

The Company is committed to maintaining a company-wide awareness of the importance of the laws and regulations of the USA PATRIOT ACT. To this end, the following anti-money laundering program has been developed:

1. Establishment of internal policies, procedures and controls.
2. Designation of compliance officer responsible for anti-money laundering program.
3. On-going employee and producer training programs.
4. Independent audit function to test the effectiveness of the anti-money laundering program.

Policies & Procedures

Policies and procedures are in place that address such areas as underwriting, cash receipts, claim payments, policy terms and compliance training. These policies provide guidance and awareness to help in determining that no Specially Designated National or citizens of a Sanctioned Country are issued a policy, paid a claim, or deposit funds and to identify potential STOLI arrangements.

Responsible Official

The Deputy General Counsel serves as AML Compliance Officer and has the overall responsibilities for the day-to-day implementation of the Anti-Money Laundering Compliance Plan. In particular, the AML Compliance Officer will perform a risk assessment and together with employees who have responsibilities for underwriting, accepting premiums, and/or paying claims, monitor the Compliance Plan.

Compliance Monitoring

The Internal Audit Department conducts regular audits of the anti-money laundering compliance programs. Results of these audits are forwarded to the AML Compliance Officer for review and management response. Employees are responsible for immediate notification of any actions not consistent with the Compliance Plan. The Compliance Officer also conducts random audits of the company's processes. In addition, sample agent business is audited each year and complaint and replacement data is scrutinized for any indication of agent misconduct.

Training for Agents

To further comply with the regulation adopted by The Financial Crimes Enforcement Network, a division of the U.S. Treasury Department, the Company has in place policies and procedures to train its agents regarding their responsibilities under the company's anti-money laundering program. The rules state that the company may satisfy this requirement by directly training its agents or by verifying that its agents and brokers have received adequate training through another insurance company or by a competent third-party. These programs are expected to be tailored to the needs of agents and to include training on identifying suspicious customer behavior and transactions as well as on procedures to report suspicious activities to the Company.

Training for Home Office Employees

All Home Office Employees regularly receive training to maintain fraud awareness, including specific training on anti-money laundering.

Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA"), was enacted for the purpose of making it unlawful for certain classes of people and entities to make payments to foreign government officials to assist in obtaining or retaining business. Specifically, the anti-bribery provisions of the FCPA prohibit the willful use of the mails or any means of instrumentality of interstate commerce corruptly in furtherance of any offer, payment, promise to pay, or authorization of the payment of money or anything of value to any person, while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to a foreign official to influence the foreign official in his or her official capacity, induce the foreign official to do or omit to do an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person. We have considered the impact of the FCPA upon the Mutual Trust business model and consider this a very low fraud risk.

Privacy Policy

The Deputy General Counsel is the individual with overall responsibility for implementation of our Privacy initiatives.

Our Privacy Policy will be communicated to our employees at the following times: initially, upon employment, via our Employee Handbook to be distributed by our Human Resource Department. Plus, each employee's manager will emphasize our Privacy requirements during the employee's training period. Thereafter, the policy will be made consistently available to all employees via the corporate portal and made part of the annual Code of Conduct Training.

Information Security & Privacy Protection Committee

The Mutual Trust Information Security & Privacy Protection Committee (ISPP) has developed a Data Security policy that is reviewed on an annual basis by all employees. The ISPP has the responsibility and authority for guiding and directing information security activities as well as for establishing and maintaining enterprise-wide information security policies, standards, guidelines, and procedures. Additionally, the ISPP will perform compliance checking to ensure that business units are operating in a manner consistent with these requirements. The ISPP has responsibility for directing and overseeing investigations of system intrusions and other information security incidents.

To be effective, information security must be a team effort involving the participation and support of every Mutual Trust employee. In recognition of the need for teamwork, this Data Security policy statement clarifies the responsibilities of users and the steps they should take to help protect Mutual Trust's information and information systems. This document describes ways to prevent and respond to a variety of threats to information and information systems including unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

Every employee at Mutual Trust, including all personnel affiliated with third parties, should comply with the information security policies found in this and related information security documents. Employees who violate this and other information security policy statements will be subject to disciplinary action up to and including termination. Users are responsible for familiarizing themselves with and complying with all Mutual Trust policies, procedures, and standards dealing with information security.

This Data Security policy applies to all computer and network systems owned by or administered by Mutual Trust, including, but not limited to, all operating systems, computers, storage devices or services, personal communication devices and application systems. Mutual Trust information along with information that has been entrusted to Mutual Trust should be protected in a manner commensurate with its sensitivity and criticality. Security measures should be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved.

Personal Information Safeguards

We limit purposeful or inadvertent access to information by our employees. Only employees who have a business reason have access to personal information about our customers. We maintain physical, electronic, and procedural safeguards to protect information. A Clean Desk Policy is in place. To assure service providers and contractors also abide by our security measures, we will add appropriate provisions to contracts we sign so as to make sure these security measures are adhered to and become contractually enforceable.

Audit

Our Audit Department undergoes in-depth fraud training. Furthermore, the Audit Department will randomly and routinely monitor our practices regarding Privacy when reviewing related topics such as Code of Conduct and Fraud. In addition, potential producer related fraudulent conduct is annually and routinely reviewed by various means such as customer complaint investigations, consumer surveys, replacement activity, persistency reports and trends, and follow-up on any reports of producer suspicious behavior. When an irregularity is discovered, a formal record of the incident, subsequent investigation findings and any subsequent disciplinary action is created and preserved. In addition, our Audit Department continually assesses our Privacy Policy in many of the matters it handles throughout the year. Any discrepancies, shortfalls and/or recommendations will be reported to the Anti-Fraud Coordinator.

Disciplinary Action

Company personnel policies require employees to follow the company's written instructions and procedures. Consistent with these policies, the Company may impose disciplinary measures for actions not in compliance with these Privacy Practices and Procedures.

Ongoing Oversight

We will adjust our policies and procedures going forward in light of new security considerations that present themselves. Furthermore, the Pan-American Life Insurance Company Anti-Fraud Coordinator shall immediately notify the Mutual Trust Anti-Fraud Coordinator of any suspected fraud involving United States Individual Life Insurance Products being administered by Pan-American Life Insurance Company. The Pan-American Life Insurance Company SIU shall routinely communicate and consult with the Mutual Trust SIU on common topics of fraud-related interests.

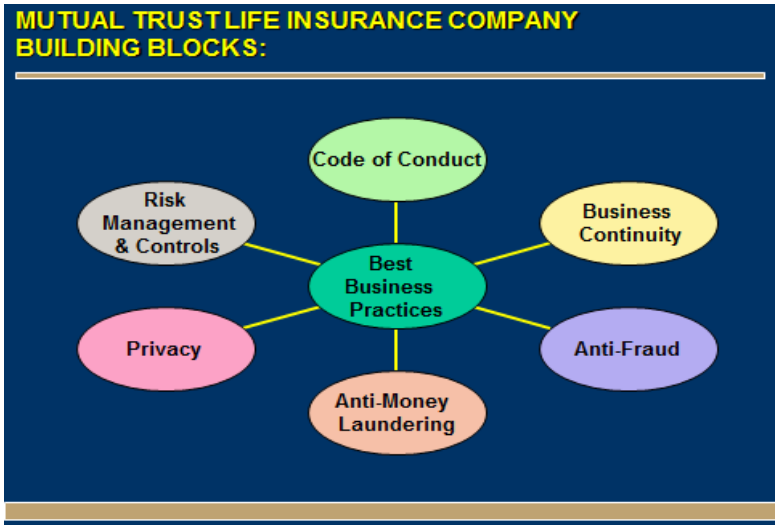
Red Flag Rules

The Company has taken steps to implement Red Flag Rules and has developed and implemented written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions Act of 2003. The program provides for the identification, detection, and response to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

Corporate Governance

The Company's legacy has shown that integrity and trust are the cornerstones to its longevity and success. The corporate governance initiatives at the Company embody the expectations, ethics, reputation, responsibility and best business practices which we as an organization wish to exemplify and hold each other accountable. We have high expectations to create an environment which embodies the qualities which have and will continue to lead us into the future.

We have several interconnecting components which demonstrate corporate governance and best business practices, as follows:



The Company has adopted a Code of Business Conduct and Ethics signed by each employee and Board of Directors' Member and covers a wide range of business practices and procedures. It is intended to set out basic principles with which we expect employees, officers and directors, to comply. Code of Conduct training is also required and covers the topics of: Conflict of Interest, Confidential Information, Use of Company Resources, Accurate Books & Records, and Privacy.

The Company has also adopted procedures to receive and respond to complaints regarding accounting, internal accounting controls, auditing or other relevant business practices. These procedures include the establishment of a confidential and anonymous way to report concerns or complaints using the Ethicspoint system, where reports may be filed either electronically or through a toll-free hot-line.

IV. ANTI FRAUD PLAN STRATEGIC COMPONENTS

A. ESTABLISHMENT OF SPECIAL INVESTIGATIVE UNIT

There is established a Special Investigative Unit ("SIU") composed of representatives from key areas of the Company. The purpose of the SIU is to investigate suspected fraudulent applications and claims by insureds or persons making claims against policies held by insureds along with any other company related fraudulent activity, deter insurance fraud and to organize the elements of the Company's integrated corporate anti-fraud strategy. The SIU has established criteria to investigate insurance fraud relating to products sold by the Company. The SIU shall cooperate with the Company's anti-fraud personnel as well as with the Company's legal personnel, Internal Audit, technical support personnel and database support personnel.

The Special Investigation Unit shall also be responsible for performing the following duties:

1. Conducting fraud investigations referred by personnel that identifies specific facts and circumstances which may lead to a reasonable conclusion that a fraud has occurred;

2. Working with the Legal Department to communicate with: 1) Fraud Divisions and 2) Law enforcement authorities;

3. Informing proper parties of fraud risks by reason of prior fraudulent activities;

4. Identifying persons and organizations that are involved in fraudulent activity;

5. Referring matters to the appropriate local authorities and agencies; and
6. Ensuring that all evidence in matters that is submitted by any person and/or entity is to be collected, identified and preserved. All email documents shall be preserved via Proofpoint software and encrypted twice. Veeam software shall be utilized to preserve Network documents while IBM's DFSMS software shall be utilized to preserve Mainframe documents. The SIU shall preserve all paper documents and files by utilizing a company approved off-site storage facility after 7 years has expired from the date any particular Fraud-related file is closed.

In regards to its on-going involvement to improve the company's ability to identify claim fraud, the SIU has oversight responsibility for the following:

1. The establishment and maintenance of systematic and effective methods to detect and investigate suspected fraudulent claims and other suspicious activity and to provide for appropriate disposition; and

2. The ongoing education and training of all claims handlers with respect to insurance fraud identification techniques, which involve matching specific claims against known patterns and trends indicating possible fraud and against specific "red flags," "red flag events" and other criteria indicating possible fraud.

Finally, the SIU is responsible for making sure the Company has established guidelines, **training** and procedures for detecting internal fraud relating to:

a. Applications;
b. Underwriting;
c. Internal Activity;
d. Agent Conduct; and
e. Claims

B. <u>EDUCATION AND TRAINING</u>

1. The SIU shall be knowledgeable of current trends regarding fraudulent insurance activity, specific "red flags," "red flag events," effective and appropriate methods of suspected fraudulent claims investigation, insurance law, the use of available resources to support the SIU's investigative activities, and any other fraudulent issues that could potentially affect the life insurance industry. The Company recognizes the indicators enumerated as an addendum to this Anti-Fraud Plan as but a few of the methodologies utilized today by both unsophisticated and sophisticated persons who would attempt to commit fraud.

The training program for all SIU members shall include a detailed program of insurance fraud awareness and education to prepare for insurance fraud and detection. Training shall include, but not limited to the following topics:

a) investigative techniques;
b) communication with applicable fraud divisions and authorized governmental agencies;
c) fraud indicators;
d) emerging fraud trends; and
e) legal and related issues.

Training shall take place each year and shall total at least 5 hours of substantive education per calendar year of the topics cited in Section IV.A. of this Handbook.

Training may also include the following topics:

a) overcharging and overpayment detection;
b) claim processing guidelines;
c) billing abuse including: duplicate bills, excessive charges, unnecessary service and/or supplies, over-utilization, services never rendered;
d) miscoded or misleading claim information;
e) hospital inpatient or outpatient billing abuse;
f) techniques for identifying abusive or fraudulent referrals and fraudulent applications for insurance coverage;
g) statutory requirements dealing with fraud referrals

SIU members shall take part in continuing education annually in the detection, investigation and proper reporting of suspected fraudulent insurance acts. The SIU shall ensure that all newly-hired employees receive an anti-fraud orientation within ninety (90) days of commencing assigned duties**.** The orientation shall provide information regarding:

a) the function and purpose of the SIU;
b) an overview of fraud detection and referral of suspected insurance fraud to the SIU for investigation;
c) a review of Fraud Division insurance fraud reporting requirements;
d) an organization chart depicting the insurer's SIU; and
e) SIU contact telephone numbers.

2 As part of its Fraud Awareness Program, the SIU shall provide ongoing anti-fraud education and training to the Company's anti- fraud personnel, which include but are not limited to claims personnel, underwriters, auditors, customer service personnel. The training provided may be provided from either internal or external sources. While SIU members receive 5 hours of training per year, the training provided to other employees will total a minimum of at least 2 hours per year.

The training shall be designed to enable employees and anti-fraud personnel to effectively analyze claims and policy information, pursue appropriate investigations, conduct appropriate and effective interviews, use available database resources, and work cooperatively with law enforcement agencies. Training will also be provided to other Company employees regarding support services essential to implementing the Company's anti-fraud plan. The following guidelines will be followed with regard to education and training:

a) Courses of instruction will be designed to address specific aspects of fraud associated with the Company's various business activities.
b) Training will include subject matter addressing ethics, false claims or other legal-related issues.
c) Courses will be designed to address the educational needs of the target personnel.
d) Anti-Fraud personnel will be presented with anti-fraud education material at the entrance level and will participate in the continuing education activities provided by the SIU.
e) Training programs may be developed and conducted either by internal personnel or by outside contractors.
f) Training programs may include but not be limited to the following modalities:

    (i) review of the function and purpose of the SIU;
    (ii) introduction/review of the written procedures established by the SIU regarding the identification, documentation and referral of incidents of suspected fraud to the SIU;
    (iii) identification and recognition of red flags or red flag events;

(iv) any changes to current procedures for identifying, documenting and referring incidents of suspected insurance fraud to the SIU; and
(v) fraud division/governmental authorities insurance fraud reporting requirements.

C. FRAUD DETECTION AND REFERRAL

The SIU is responsible for coordinating the detection, referral and investigation of suspected fraudulent situations. The SIU has adopted a Fraud Detection Procedures Manual that has been distributed to all integral employees so as to assist in the identification, detection and handling of suspicious insurance activities.

Using guidelines established by the SIU, trained anti-fraud personnel are responsible for the early detection of suspicious or fraudulent acts. All employees shall report any suspicious information and/or possible fraudulent event to their immediate supervisor. The Company has also established an anonymous hotline to facilitate this initial reporting. Supervisors shall then examine all readily available information in order to determine if this matter should be reported to the Anti-Fraud Coordinator for SIU consideration. If possible under the circumstances, this decision should be made within 30 days of reporting of suspicious activity. In order for an appropriate evaluation of each matter it is vital for all staff to:

1. Report allegations swiftly;
2. Identify and record all evidence that has been received;
3. Ensure that evidence is sound and adequately supported; and
4. Make secure all of the evidence has been collected and is preserved.

As part of the Anti-Fraud Coordinator's analysis, a comparison of the suspected insurance fraud activity or transactions against:

1. Patterns or trends of possible fraud;
2. Fraud Indicators ("Red flags");
3. Events or circumstances present on the claim or suspicious activity;
4. Behavior or history of person(s) submitting a claim, application or suspicious item; and
5. Other criteria that may indicate possible fraud.

The SIU shall accept reports of suspected fraud from any source within or outside the Company. The SIU shall review the submitted report concerning the suspected fraud and should be provided with as much information concerning the allegation as possible, such as:

1. A complete description of the alleged fraud and/or wrongdoing;
2. The alleged connection to the Company (i.e. vendor, agent, policy holder, etc.);
3. The names and locations of the persons or entities involved;
4. The approximate dates or time frame of the transactions or alleged fraudulent event;

5. An approximate amount of funds at risk;

6. The location and description of any potentially relevant documents, data or records; and

7. The names and locations of other persons who may have information regarding the alleged misconduct and are willing to provide it to the Company.

Once the SIU is notified of possible fraudulent activities, the SIU will promptly:

1. Confirm the alleged wrongdoing involves the Company;

2. Notify the Legal Department and Internal Audit; and

3. Prepare an initial investigative plan, including the names of personnel who will work on the case and any outside resources needed. Outside sources can include, but are not limited to industry-recognized databases such as TransUnion Direct, LexisNexis, State Department of Corrections, Motor Vehicle, Social Security Death Master, and General Internet searches along with database capabilities provided by various Trade Associations such as LIMRA and the ACLI.

Once these preliminary steps are taken, the SIU, in conjunction with the Legal department and Internal Audit shall conduct a thorough investigation into the suspicious claim/application or other item. Once the investigation is complete the SIU may, if it deems necessary, provide notice to the local authorities indicating a violation is suspected on the basis of fraud factors and/or indicators, but that sufficient evidence has not been developed in which to submit a full referral to the local authorities.

An investigation shall be considered complete when:

1. All reasonable and appropriate investigative leads have been exhausted;

2. An investigation has identified a pattern of possible violations; or

3. When one or more violations included in the identified pattern has been investigated and corroborated; and

4. Findings have been recorded in writing together with final recommendations and reasons for recommendation.

If the SIU establishes a reasonable belief that fraud has been committed, the SIU shall immediately notify the appropriate state insurance department or governing authority of the fraudulent occurrence. All notifications to state insurance departments or other governing authorities shall meet all state mandated time deadlines for such notifications, including, but not limited to, California's 60-day notification requirement. The Company shall utilize a state's electronic reporting system along with any other alternative means available to report suspected fraud. The Company shall maintain a record of the date that the suspected fraud was identified along with the date that it reports any such activity to the Insurance Department or other governing authority. Upon completion of an investigation in which the following criteria is met, the Legal Department on behalf of the SIU will complete all applicable referral forms and refer the matter and/or case to the local authorities for further investigation or other appropriate actions.

1. Any application or claim where the facts and circumstances create a reasonable suspicion that a person or entity fraudulent act has occurred;

2. There is sufficient independent evidence corroborating the reasonable suspicion from which a person could reasonably conclude that a person or entity has entered into a fraudulent act. This includes:
    a. Statement from a witness;
    b. Documentary evidence that directly negates a material element of the claim or directly establishes the falsity of a material element of an insurance application;
    c. An expert report; and
    d. Any other apparent misrepresentations tending to negate a possibility that the misrepresentation was merely an error.

If any Company employee becomes aware of fraud involving employee misconduct, the employee shall report his suspicions to the anonymous hotline, directly to the Internal Audit Department or to an officer within the Legal Department.

D. FRAUDULENT CLAIM INVESTIGATION

Once assigned responsibility for investigation of a suspicious claim, the SIU will conduct an investigation regarding the claim. The SIU shall develop guidelines and procedures for the conduct of its investigations, which shall include the following:

1. The SIU shall establish a case file with regard to the suspected fraudulent claim;

2. The SIU shall preserve all relevant documents and property related to the investigation;

3. The SIU shall conduct a thorough review of the case file as well as the Complaint Log for other complaints involving the same person or service provider. If other cases are found, the SIU will obtain all information concerning those cases;

4. The SIU shall review all pertinent background information received from the referring source;

5. The SIU shall develop information as needed, to include:
    a. Claim fraud data sheets
    b. Claims copies
    c. checks and/or payment vouchers
    d. explanation of benefits and/or policy provisions
    e. the identification of all potential witnesses who may provide relevant information on the truth or falsity of the claim;

6. The SIU shall check for processing or clerical errors. If a determination is made that the suspected fraudulent claim resulted from a processing or clerical error, the SIU will close the case and advise the referring party as well as all individuals contacted with regard to the case;

7. If the SIU is satisfied that sufficient grounds exist to consider the claim as being fraudulent, the SIU shall prepare a concise summary of the completed investigation, setting forth the SIU's conclusion(s) regarding the suspected fraudulent claim and the basis for said conclusions;

8. In conjunction with the Legal Department, the SIU shall preserve the confidentiality of all related documents. SIU shall also make sure that all communications and documents are properly maintained in the file;

9. Upon completion of an investigation, the SIU shall prepare a concise summary report of the completed investigation setting forth the investigators' conclusions regarding the suspected fraud and the basis for such conclusion. This report shall also include a recommendation in

writing to the Claims departments or other relevant departments, to either pay or deny the claims with reasons. The report should contain certain information such as:

a) Fraud and referral type
    (i) Fraud type
b) New referral/amended referral indicator
c) Reporting party information
    (i) Reporting party type
    (ii) Reporting party name
    (iii) Reporting party ID number
    (iv) Reporting self-insured/contracted third party license number, as appropriate
    (v) Reporting party address, city, state and zip code
    (vi) Reporting party email address (generally, contact address)
d) Alleged victim information, as appropriate
    (i) Alleged victim company name
    (ii) Alleged victim California Company number
    (iii) Alleged victim self-insured number
    (iv) Alleged victim address, city, state and zip code)
e) Insurance policy or claim information, as appropriate
    (i) Claim number associated with referral
    (ii) Insurance policy number associated with referral
    (iii) Date of loss or injury
    (iv) Geographic location where loss or injury occurred
    (v) Insurance premium dollar loss
    (vi) Total potential loss on claim prior to the identification of fraud
    (vii) Total claim loss paid to date
    (viii) Actual suspected fraudulent loss amount paid to date
    (ix) A complete synopsis of all the facts on which the reasonable belief of the insurance fraud is based.
f) Other agency referral information, as appropriate
    (i) Names of other authorized governmental agencies receiving this referral
    (ii) Names of any District Attorney's Office receiving this referral
    (iii) National Insurance Crime Bureau (NICB) referral indicator
    (iv) The names of any other agencies receiving this referral
g) Referral contact information, as appropriate
    (i) Referral contact name and phone number
    (ii) Claim or case file handler and phone number
    (iii) Name and phone number of person who completed referral
    (iv) Date referral was completed
h) Information for each party associated with the referral
    (i) Identification of the role of the party to the loss
    (ii) Phone number
    (iii) Address, city, state and zip code
    (iv) Date of birth or age
    (v) Social security number
    (vi) Tax identification number
    (vii) Drivers license number
    (viii) State of party's driver’s license
    (ix) Vehicle license plate number
    (x) Vehicle license plate state
    (xi) Vehicle identification number
    (xii) Other names or identifiers used by the party
    (xiii) Claim of injury indicator.

The SIU, with assistance of the Legal Department, will determine on a case-by-case basis which cases are referred to government authorities and/or law enforcement. The Anti-Fraud Coordinator shall maintain the written policy for reporting such cases and shall be available for inspection by all Insurance Administrations, including the Maryland Insurance Administration.

Termination

If an investigation results in a recommendation to terminate, the recommendation will be reviewed for approval by the appropriate company officers before any such action is taken.

Best Practices Committee

The purpose of the Best Practices Committee is to act as an advisory committee charged with maintaining, monitoring and improving the Company's policies and procedures that make up the commitment to ethical market conduct.

The Committee is represented by individuals from Compliance, Internal Audit, Legal, Marketing and Administration Client Services. This cross discipline approach to the committee formation brings together a breadth of experience and depth of knowledge to respond to market conduct, regulatory, compliance and other issues facing the life insurance industry as well as the Company.

The trend in legal liability and attitudinal shifts continues to impact the importance of sound ethical market conduct practices and procedures. Recent changes in the law and the way states regulate have increased the responsibilities of life insurers. The Best Practices Committee continually coordinates, monitors or reviews market conduct issues. The Committee has responded by endorsing:

- training sessions on ethical practices and fraud awareness
- the production and distribution of the Guide to Business Practices and the Anti-Fraud Handbook
- quality business reviews
- the development of Best Practices Guidelines

Annual Reporting

Certain states require insurance companies to provide an Annual Report summarizing the company's anti-fraud activity annually. Mutual Trust files such Annual Reports as required addressing fraud activity, policies and procedures. Furthermore, other states require the filing of reports utilizing specific data formats. Mutual Trust strictly complies with all state reporting requirements. Mutual Trust retains records of all anti-fraud initiatives.

APPENDIX I

FRAUD DETECTION PROCEDURES MANUAL

I. DUTIES AND FUNCTIONS OF THE SPECIAL INVESTIGATIONS UNIT

The main purpose of the SIU is to investigate suspected fraudulent claims and other fraudulent activity, deter insurance fraud, and to organize the elements of the Company's integrated, corporate anti-fraud Strategy.

The SIU has oversight responsibility for the following anti-fraud activities relating to fraudulent insurance claims:

1. The establishment and maintenance of methods to detect and investigate suspected fraudulent claims and to provide for appropriate disposition; and

2. The ongoing education and training of all claims handlers with respect to insurance fraud identification techniques, which involve matching specific claims against known patterns and trends indicating possible fraud and against specific "red flags," "red flag events" and other criteria indicating possible fraud.

The Special Investigations Unit shall also be responsible for performing the following duties:

1. Conducting investigations of claims and/or applications referred by personnel that identifies specific facts and circumstances which may lead to a reasonable conclusion that a violation has occurred;

2. Retaining information regarding fraudulent claims and applications, which contain: the name, address and any other relevant information regarding the parties involved in the investigation;

3. Work with the Legal Department to serve as a liaison to and manage all communications with: 1) the Fraud Divisions of the Insurance Departments for those states where the Company is a licensed insurer and 2) law enforcement authorities in those states where the Company is a licensed insurer;

4. Informing proper parties of risks by reason of prior fraudulent activity;

5. Identifying persons and organizations that are involved in suspicious claim activity and application fraud;

6. Working with the Legal Department to refer matters to the appropriate local authorities and agencies by providing the corresponding notices; and

7. Ensuring that all evidence in matters that is submitted by any person and/or entity is to be collected, identified and preserved.

In addition, the SIU is responsible for establishing guidelines and procedures for detecting internal fraud relating to:

a. Applications;
b. Underwriting;
c. Office Activities;
d Claims; and
e. Agent Conduct.

II. ANTI-FRAUD GUIDELINES FOR LIFE AND ANNUITY BUSINESS

Claims

All claims with regard to an individual life insurance policy are reviewed by claims processors within the Claims Department. A claims processor reviews all claims against the Company's internally published "red flag" indicators. In the event that a red flag indicator exists with regard to a claim, the claims processor advises the Claims Manager. If in the view of the Claims Manager the claim warrants further review for possible fraudulent content, the Company's Anti-Fraud Coordinator is notified. The Anti-fraud Coordinator will report the matter to the SIU, as needed. Upon recommendation of SIU personnel, the claim may be placed under a preliminary investigation.

Mutual Trust requires the following initial documentation with regard to any death claim:

a. Death Certificate
b. Claim Form
c. Accident Report and/or Coroner's Report, and newspaper clippings as appropriate
d. Witness and Law Enforcement Statements and Interviews as appropriate
e. Any other investigative documentation needed to approve the claim.

If a death benefit claim is placed under preliminary investigation, the Company may take any of the following steps, depending on the nature of the red flag.

a. For claims within the contestable period, the Company may obtain the medical records of the insured and review them to determine if fraudulent representations were made in the application with regard to the health of the insured.
b. For death claims outside the United States, the Company may contract with a special investigator to verify the death (and to the extent possible the cause of death) of the insured.

The Claims Department is the lead business unit responsible for the prevention, detection and investigation of claims fraud. All Claims Forms used by the Claims Department contain the anti-fraud disclaimers required by the laws and regulations of the state in which the Claims Form is used. Claims fraud includes but is not limited to:

- Submission of a false claim in any manner;
- Alteration of legal documents such as death certificates, affidavits, etc.;
- Providing false information regarding the claimant;
- Offering or providing anything of material value to any Company officer or employee or General Agent or Agent in exchange for special consideration in the claims process; and
- Any similar or related irregularity.

Potential Red Flags for claims fraud include:

- Any deaths within the contestable period;
- High dollar policies;
- Any question whether the insured knew about a policy;
- Deaths where a body is not recovered;
- Discrepancies in claims documents;
- Questionable causes of death;
- Multiple policies not requiring medical exams; and
- Changes to a policy's limits and coverage.

If there is a question as to whether an action constitutes fraud, the Anti-Fraud Coordinator must be contacted.

Application and Underwriting

The Underwriting Department along with Mutual Trust's independent producers are the ones primarily responsible for the detection and prevention of underwriting fraud. Underwriting and/or Application fraud includes but is not limited to:

- Applicants refusing to provide accurate personal information;
- Applicants failing to provide accurate information as it relates to the purchase of other policies; and
- Applicants providing inaccurate heath information on Company applications.

Potential Red Flags for Application and Underwriting Fraud include:

- Applicant states that he/she will soon be moving to the insuring state;
- Applicant is in a hurry to secure coverage;
- Applicant attempts to pay premium with cash or some other untraceable method;
- Applicant requests that all correspondence be sent to out of state address;
- Applicant has no driver's license or out of state license;
- Applicant is unusually familiar with insurance terms;
- Purchase is inconsistent with client needs;
- Inconsistent signature on application when compared to other documents;
- Applicant has no concern for performance of the policy;
- Applicant's home telephone number is disconnected;
- Mail sent to the applicant is returned due to a bad address; and
- The applicant, unsolicited, walks into producer's office to apply for a policy and was not referred to the producer by another policyholder.

If there is a question as to whether an action constitutes fraud, the Anti-Fraud Coordinator must be contacted.

Agent

While Mutual Trust's independent producers remain a key component in the company's ability to identify and fight against fraud, their relationship with the client and the company creates a unique opportunity for potential abuse and fraudulent behavior. Examples of Agent Fraud include but are not limited to the following:

- Failure to comply with all federal, state and local laws and regulations including insurance laws and regulations;
- Having any improper or illegal financial dealings or failure to exercise fiduciary responsibility to the Company, any policyholders of the Company, or any other person;

- The payment of any commission to an unlicensed agent;
- Deliberate omission or falsification of applicant history or information whether done by the applicant or agent administering the application process;
- Forgery or unauthorized alteration of the Company applications used in making underwriting decisions;
- Fraudulent alteration, addition or removal of policyholder or insured information on the Company management information systems;
- Offering or providing anything of material value to any Company employee in exchange for special consideration in the application or underwriting process;
- False or fraudulent representations, including false advertising regarding the Company policies made to applicants by agents of the Company;
- Any fraud or impropriety involving agent commissions;
- The withholding, theft, misappropriation or fraudulent conversion of premiums paid by applicants or insureds;
- The improper conversion of claims payments;
- Any similar or related irregularity, including "churning" or “twisting”; and
- Borrowing from customers, policyholders, clients, or beneficiaries.

Potential Red Flags for Agent Fraud include:

- Misrepresentations on applications submitted;
- Minimum premium paid on initiation of policy;
- High lapse rates;
- Payments made by cash or cash equivalents;
- Application is not complete;
- Mail sent to insured’s address is returned;
- Insured works in another state; and
- Insured has an out of state license.

If there is a question as to whether an action constitutes fraud, the Anti-Fraud Coordinator must be contacted.

Home Office

Allegations of possible Home Office frauds should be reported to the Anti-Fraud Coordinator. The Anti-Fraud Coordinator will interview the reporting party to assess the nature of the allegations and obtain the names of all suspects. The Anti-Fraud Coordinator will detail the extent of evidence available to support the alleged occurrences. The reporting party will be instructed not to discuss the matter with anyone unless specifically requested to do so by the Anti-Fraud Coordinator or his/her designee.

The terms insurance fraud and other irregularities include but is not limited to:

- Any dishonest or fraudulent act or attempted act by employees of the Company.
- Forgery or alteration of any document relating to the Company’s insurance policies or insured parties.
- Forgery or alteration of checks, bank drafts, or any other financial documents.
- Fraudulent alteration, addition or removal of information on the Company’s management information systems.
- Misappropriation of funds, securities, supplies, computers, or other assets.
- Improprieties in the handling of monies or reporting of financial transactions.
- Public disclosures of confidential policyholder information such as medical information, cause of death, financial data, etc. without appropriate approval.
- Disclosing to other persons the confidential or private business activities of the Company.
- Accepting or seeking anything of material value from applicants, beneficiaries, Agents or other

interested parties in exchange for special consideration in the application, underwriting or claims process.

- Unauthorized destruction, removal or conversion of records, furniture, fixtures, and equipment, or assets belonging to the Company.
- The improper withholding of any money or premiums paid on an insurance policy, if the insurance contracted for is not ultimately provided.
- Any false statement made to law enforcement agencies, prosecutors or the insurance departments of any state.
- Any similar or related irregularity.

Potential Red Flags for theft and fraud occurring in the Home Office include:

- Duplicate payments;
- Missing Documents;
- Holes in accounting records;
- Employees maintaining the same address as a vendor;
- Employees who consistently work overtime and refuse to take a vacation;
- Unusual changes in behavior and work habits; and
- Possessiveness about work duties.

If there is a question as to whether an action constitutes fraud, the Anti-Fraud Coordinator must be contacted.

III. FRAUD DETECTION AND REFERRAL

The SIU is responsible for coordinating the detection, referral and investigation of suspected fraudulent situations. All employees shall report any suspicious information and/or possible fraudulent event to their manager. That manager shall then examine all readily available information in order to determine if this matter should be reported to the Anti-Fraud Coordinator. The Anti-Fraud Coordinator will report the matter to the SIU for future investigation and handling. The Legal Department and Internal Audit will be consulted, if necessary during this examination stage. If possible under the circumstances, this decision should be made within 30 days of receipt of the notice of the suspected fraudulent behavior. In order for an appropriate evaluation of each matter it is vital for all staff to:

1. Report allegations swiftly;
2. Identify and record all evidence that has been received;
3. Ensure that evidence is sound and adequately supported;
4. Make secure all of the evidence has been collected and is preserved. All email documents shall be preserved via Proofpoint software and encrypted twice. Veeam software shall be utilized to preserve Network documents while IBM's DFSMS software shall be utilized to preserve Mainframe documents. The SIU shall preserve all paper documents and files by utilizing a company approved off-site storage facility after 7 years has expired from the date any particular Fraud-related file is closed.

All reports shall include:

1. Referral contact name, title, and phone number
2. Claim or case file handler and phone number
3. Name and phone number of person who completed referral
4. Date referral was completed (not required if submitted electronically)

As part of his review, the manager shall compare the suspected insurance fraud activity or transactions against:

1. Patterns or trends of possible fraud;

2. Fraud Indicators (“Red flags”);
3. Events or circumstances present on a claim;
4. Behavior or history of person(s) submitting a claim or application; and
5. Other criteria that may indicate possible fraud. Other criteria can include, but are not limited to industry-recognized databases such as TransUnion Direct, LexisNexis, State Department of Corrections, Motor Vehicle, Social Security Death Master, and General Internet searches along with database capabilities provided by various Trade Associations such as LIMRA and the ACLI.

The Anti-Fraud Coordinator and SIU shall accept reports of suspected fraud from any source within or outside the Company. The SIU shall review the submitted report concerning the suspected fraud and should be provided with as much information concerning the allegation as possible, such as:

1. A complete description of the alleged fraud and/or wrongdoing;
2. The alleged connection to the Company (i.e. vendor, provider, policy holder, etc.)
3. The names and locations of the persons or entities involved;
4. The approximate dates or time frame of the transactions or alleged fraudulent event;
5. An approximate amount of funds at risk;
6. The location and description of any potentially relevant documents, data or records;
7. The names and locations of other persons who may have information regarding the alleged misconduct and are willing to provide it to the Company.
8. Identity of any relevant person and their role of the party to the loss.

Once the SIU is notified of a possible fraudulent application or claim the SIU will promptly:

1. Confirm the alleged wrongdoing involves the Company;
2. Notify Legal Department and Internal Audit; and
3. Prepare an initial investigative plan. The plan shall include personnel to be assigned and possible outside resources needed to undertake this investigation.

Once these preliminary steps are taken, the SIU shall conduct a thorough and ethical investigation into the suspicious claim/application. Once the investigation is complete the SIU may if it deems necessary provide notice to the local authorities indicating a violation is suspected on the basis of fraud factors and/or indicators, but that sufficient evidence has not been developed in which to submit a referral to the local authorities.

An investigation is completed ethically and in Good Faith when:

1. All reasonable and appropriate investigative leads have been exhausted;
2. An investigation has identified a pattern of possible violations; or
3. When one or more violations included in the identified pattern has been investigated and corroborated;
4. SIU findings have been recorded in writing together with its final recommendations and reasons for recommendation. The findings shall be summarized in the form of a written report addressing all aspects of the investigation along with accompanying evidence serving as the basis of any objective conclusions reached from the investigation. The report shall clearly spell out dates and order of the investigation so as to be suitable and beneficial for courtroom testimony.

The SIU shall be responsible for writing a concise and complete summary of the entire investigation, which is specific to the investigation at hand, is separate from any other document prepared in connection with the

investigation, and includesing the investigators's findings regarding the suspected insurance- fraud and the basis for their findings. The summary shall answer the following questions:

The summary shall include the following information, if known:

1. The facts that caused the reporting party to believe insurance fraud occurred or may have occurred.
2. The suspected misrepresentations and who it was that allegedly made them.
3. How the alleged misrepresentations are material and how they affect the claim or insurance transaction.
4. Identification of pertinent witnesses to the alleged misrepresentation.
5. What documentation there is of the alleged misrepresentation.

In addition, the summary prepared shall include a statement as to whether or not the investigation is complete.

If the SIU establishes a reasonable belief that fraud has been committed, the SIU shall immediately notify the appropriate state insurance department or governing authority of the fraudulent occurrence. All notifications to state insurance departments or other governing authorities shall meet all state mandated time deadlines for such notifications, including, but not limited to, California's 60-day and Kentucky's 14-day notification requirement. Upon completion of an investigation in which the following criteria is met, in conjunction with the Legal Department, the SIU will complete all applicable referral forms and refer the matter and/or case to the local authorities when the investigation is completed for further investigation of other appropriate actions.

1. Any application or claim where the facts and circumstances create a reasonable suspicion that a person or entity fraudulent act has occurred;
2. There is sufficient independent evidence corroborating the reasonable suspicion from which a person could reasonably conclude that a person or entity has entered into a fraudulent act. This includes:

    a. Statement from a witness;
    b. Documentary evidence that directly negates a material element of the claim or directly establishes the falsity of a material element of an insurance application;
    c. An expert report; and
    d. Any other apparent misrepresentations tending to negate a possibility that the misrepresentation was merely an error.

If any Company employee becomes aware of other types of fraud involving or affecting the Company, other than insurance claim fraud, the employee shall report his suspicions directly to the anonymous hotline, Internal Audit Department or to an officer within the Legal Department.

IV. RECOVERY/LITIGATION/PROSECUTION

In instances where suspicions regarding fraudulent claims have been corroborated as a result of an investigation, the SIU shall refer to the Legal Department for a decision to seek restitution, if deemed economically feasible, or to seek prosecution via referral to law enforcement and introduction to the State or Federal judicial system. The Company retains the prerogative to handle the issue via a mechanism which allows for non-payment of claim, restitution or some other effective method of recovery; or to refer the matter to the appropriate prosecutorial body for introduction into the court system.

In the case of an employee or agent fraudulent act, the case will be referred by the Legal Department to the Company's or the agent's fidelity bond carrier.

V. COOPERATION AND ACCESS

The SIU shall cooperate with the Fraud Units/Divisions of the various Insurance Departments and other relevant law enforcement agencies and authorized governmental agencies to assure compliance with all pertinent insurance statutes and regulations and provide a prompt response to requests made in the course of any criminal or civil investigation undertaken by authorized governmental agencies or law enforcement. Such cooperation includes access to the Company's offices upon reasonable notice and at reasonable hours to verify compliance with this Anti-Fraud. Furthermore, the company shall maintain appropriate records for all Insurance Administrations to determine the effectiveness of its anti-fraud plan and strategies.

Your plan must state that its reporting policy is in writing and maintained in the office of the company point of contact for fraud and must be available for inspection by the Maryland Insurance Administration.

APPENDIX II

SIU COMMITTEE MEMBERS

The Special Investigative Unit of Mutual Trust Life Insurance Company shall consist of the following individuals:

SIU Member Name	Department	Telephone Number & Email Address
Rod Gross	Internal Audit VP, Internal Audit	(630) 684-5366 grossr@mutualtrust.com
Fred Medrano	Director, Underwriting	(630) 684-5438 medranof@mutualtrust.com
Enrique Monzon	Claims Global Chief Claims Officer	(504) 566-3648 ERmonzo@palig.com
Stacy McWhorter	Administration VP, Life Operations	(630) 684-5593 mcwhorters@mutualtrust.com
Cheryl Puziss	Legal Sr. Paralegal	(630) 684-5422 puzissc@mutualtrust.com
John Seneczko	Legal Anti-Fraud Coordinator	(630) 684-5481 seneczkoj@mutualtrust.com

APPENDIX III

KEY CONTACTS

There are several ways to contact an appropriate, authorized individual concerning a fraud matter.

In person, by mail, by telephone:

Mailing Address:
Mutual Trust Life Insurance Company, A Pan-American Life Insurance Group Stock Company
1200 Jorie Boulevard
Oak Brook, IL 60523

Main Telephone Number:
630-990-1000

Contact:
Anti-Fraud Coordinator

Corporate Website:
https://www.mutualtrust.com/about/copyrightnotice.asp