ANTI-FRAUD HANDBOOK

2012 Update

Mutual Trust Financial Group (Company) recognizes that an insurance company must take a proactive, as well as a reactive, stance against fraud in today's business environment.

An anti-fraud plan serves the following purposes:

- To communicate to all stakeholders the policies and procedures in place that will help to deter application, underwriting and claims fraud as well as Home Office or external frauds, violations of laws and regulations or other improprieties.

- To identify the persons within the Company responsible for fraud prevention, detection and investigation.
- To detail the management procedures in place for preventing, detecting, investigating, monitoring and responding to potential fraudulent situations.
- To comply with the regulatory laws impacting the life insurance industry.
- To be a part of a corporate governance program.

Anti-Fraud Awareness Program

The effectiveness of the anti-fraud awareness program at the Company is measured by the following:

- Audit Committee Corporate Governance Oversight
- "Tone at the Top" Senior Leadership
- Existence of this Anti-Fraud Handbook
- Periodic anti-fraud program assessments
- An active Best Practices Committee
- The effectiveness of the Company's preventive and detective controls
- The implementation and effectiveness of positive pay feature over cash disbursements
- The Company's ability to comply with all regulatory and compliance requirements
- Education and awareness training, including anti-money laundering
- Accounting, auditing and NAIC requirements to review the appropriateness of fraud controls

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

Section I - Responsibilities

Home Office

All officers and employees of the Company are responsible for preventing and detecting insurance fraud and other irregularities. The management of the Company is responsible for maintaining procedures that would reasonably deter such wrongful acts. All officers and employees of the Company 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.

Anti-Fraud Coordinator

The Anti-Fraud Coordinator, who is also the Vice President, Internal Audit, is responsible for the continued maintenance of this anti-fraud plan, 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.

Deputy General Counsel

The Deputy General Counsel is responsible for reviewing and monitoring 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, and registered representatives (in coordination with the Compliance Officer for MTL Equity Products), 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.

Investigative Responsibilities

The Anti-Fraud Coordinator has the primary responsibility for coordinating the investigation of Home Office and external fraud allegations at the Company. Depending on the nature of the allegations, the Anti-Fraud Coordinator in coordination with the Deputy General Counsel may choose to engage the assistance of outside legal counsel, outside Special Investigations Unit (SIU) and/or appropriate law enforcement authorities.

If the investigation reveals that fraudulent activities have occurred, the Anti-Fraud Coordinator or his/her designee will notify the Deputy 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.

Confidentiality
The Anti-Fraud Coordinator or Deputy General Counsel, if appropriate, is responsible for receiving relevant information on a confidential basis from an employee, policyholder, insured, General Agent, writing agent, registered representative (in coordination with the Compliance Officer for MTL Equity Products), or third party who suspects dishonest or fraudulent activity. The individual providing information should contact the Anti-Fraud Coordinator, or Deputy General Counsel, if appropriate, 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.

Special Investigations Unit (Independent)
Based upon the nature of each case, an independent, third party Special Investigations Unit may be referred to for further investigation. The SIU will either conduct the investigation itself or recommend properly licensed investigative subcontractors in to assist in the investigation as appropriate.

The independent, third party SIU is utilized for the investigation and identification of potential fraudulent activity committed by customers, agents, employees, or any other party in conjunction with the Company's normal services and processes that are consistent with every day insurance operations.

Scope of Responsibilities
The conditions of this program apply to any irregularities, or suspected irregularities, involving not only employees of the Company but also vendors providing goods and services to the Company's insureds, clients, outside agencies and investigators.

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position, title, or relationship with MTL.

General Agents, Writing Agents, and Registered Representatives
The Company recognizes that General Agents, Writing Agents, and Registered Representatives are independent business persons representing insureds and potential insureds, and are not employees of the Company. However, the Company expects all independent agents and registered representatives 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, Writing Agents, and Registered Representatives, and will take appropriate steps as warranted.

All General Agents and their agents, registered representatives, and employees are the Company's partners in the prevention and detection of insurance fraud and other irregularities. All General Agents, their agents, registered representatives, 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 and their agents, registered representatives, 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, registered representatives (in conjunction with the Compliance Officer for MTL Equity Products), and employees must be reported to the Company's Deputy General Counsel who will coordinate the appropriate action with 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 General Agent and Registered Representative appointments. The application process includes a background check that may include inquiries to state insurance regulators. The Company also verifies that the General Agent has the appropriate licenses and qualifications in the necessary state(s). The General 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.

General Agents and Registered Representatives are encouraged to visit the MTL agent website to review this Anti-Fraud Handbook, as well as the *Guide to Business Practices*. Agents and Registered Representatives 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 and Registered Representative 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.

Section II – Home Office Policies and Procedures

The Company has adopted numerous Corporate Policies intended to identify 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) Agent and 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:

- 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;
- Assess the awareness level of the existing anti-fraud program and plan in all departments;
- Determine whether the overall anti-fraud program in place remains accurate, relevant and effective; and
- Assure compliance with all regulatory and legal requirements.

Section III - 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, producer, and registered representative 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 Compliance Director 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 Deputy General Counsel for review and management response. Employees are responsible for immediate notification of any actions not consistent with the Compliance Plan**.**

Training for Agents and Brokers

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 and brokers 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 and brokers 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 brokers 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 attend education and 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 persons 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 MTL business model and consider this a very low fraud risk.

Section IV - Privacy

Information Security & Privacy Protection Committee

The MTL Information Security & Privacy Protection Committee (ISPP) has developed a Data Security policy that is reviewed and acknowledged 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.

MTL Team Effort

To be effective, information security must be a team effort involving the participation and support of every MTL 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 MTL’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

Every employee at MTL, 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 MTL policies, procedures, and standards dealing with information security.

Systems

This Data Security policy applies to all computer and network systems owned by or administered by MTL, including, but not limited to, all operating systems, computers, storage devices or services, personal communication devices and application systems. MTL information, and information that has been entrusted to MTL 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.

Procedures

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 these security measures enforceable events.

Responsible Official

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.

Audit

Our Audit Department will routinely monitor our practices regarding Privacy when reviewing related topics such as Code of Conduct and Fraud. 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 Deputy General Counsel.

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.

Red Flags Rules

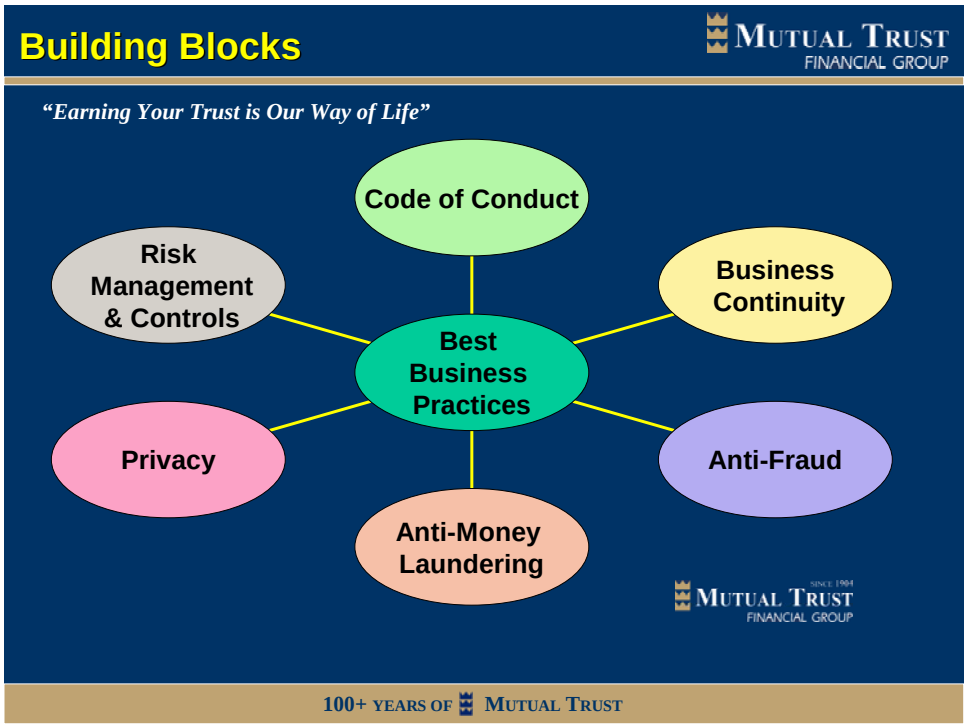
The Company has taken steps to implement Red Flags Rules and has developed and implemented written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions Act of 2003. The program provides for the identification, detection, and response to patterns, practices, or specific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

Section V – Code of Conduct

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.

Section VI - Fraud Detection

All officers and employees of the Company have the responsibility to recognize potential claims fraud and application fraud. As noted in Section II. Fraud Prevention and Detection Policies and Procedures for Home Office, all Company officers 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 must be reported to the Anti-Fraud Coordinator.

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.

Actions Constituting Fraud, Home Office:

The terms insurance fraud and other irregularities refer to, but are 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, General 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.

Application and Underwriting

- The payment of any commission to an unlicensed agent.
- 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's management information systems.
- Any fraud or impropriety involving agent commissions.

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

Claims and Application

The Underwriting department is the lead business unit responsible for the detection and prevention of underwriting fraud. 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.

If a claims fraud, underwriting fraud, or any other irregularity by an insured, beneficiary or third party is alleged or suspected, the Anti-Fraud Coordinator will establish an investigative work plan to determine the methodology of investigating the allegations. The work plan may consist of a documentary review of the Company's internal records, the records of the General Agent or Agent, public record filings and the records of the insureds. The work plan may also consist of interviews of the General Agents, Agents, policyholders, insureds, and other persons deemed appropriate. If the investigation reveals that fraudulent activities have occurred, the Anti-Fraud Coordinator or his/her designee will notify proper executives, legal counsel and, if appropriate, the Company's Board of Directors.

Underwriting and Claims

- Failure to properly follow company procedures regarding compliance to the Office of Foreign Assets Control (OFAC).
- Deliberate omission or falsification of applicant history during the application process.
- 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 application or claims process.
- Any similar or related irregularity.

Agents and Registered Representatives

- 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 or registered representatives of the Company.
- Any fraud or impropriety involving agent commissions.
- The withholding 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”.
- Prohibit lending to or borrowing from customers, policyholders, clients, or beneficiaries.

Section VII - Administration

The Anti-Fraud Coordinator is responsible for the continued maintenance of this anti-fraud plan, the prevention and detection of Home Office fraud and the coordination of any investigation of suspected frauds, both internal and external. All irregularities detected or suspected must be reported to the Anti-Fraud Coordinator or his/her designee.

Authorization for Investigating Suspected Fraud

In those instances in which the Anti-fraud Coordinator believes it to be in the best interest of the Company, he/she has the authority and duty, after consulting with appropriate executives, to:

- Take control of, and/or gain full access to all Company premises, whether owned or rented; AND
- Examine, copy, and/or remove all or any portion of the contents of the Company files, desks, cabinets, computers and other storage facilities on the premises without prior knowledge or consent of any individual who may use or have use of any such items or facilities in accordance with applicable local, state, and federal laws.

Reporting Procedures

Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

Any person reporting a suspected fraud must adhere to the following restrictions:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case with any Company employee or insured other than the Anti-Fraud Coordinator, his/her designee, legal counsel, or individuals within MTL who have a legitimate "need to know."
- Do not discuss the case, facts, suspicions, or allegations with anyone outside of the Company unless specifically asked to do so by the Anti-Fraud Coordinator or legal counsel.
- Refer all press and outside inquiries to the Anti-Fraud Coordinator.
- All services of process are to be referred to the Anti-Fraud Coordinator or legal counsel.

Fraud Plan

The Anti-Fraud Handbook presents a set of procedures that the Company undertakes when there are allegations or evidence of possible Home Office fraud, fraud by General Agents or Agents and fraud by claimants or insureds. These procedures will be used as a guideline, and may be modified at management's discretion. The Company recognizes that each possible fraud situation is different and management responses can and will vary.

The Anti-Fraud Coordinator will determine if the allegations of fraud can be easily verified through a review of accounts, files, or system data. The Anti-Fraud Coordinator will consider taking measures, such as data-backups or securing workstations, to protect documents and records that may be relevant to the fraud allegations. The Anti-Fraud Coordinator and another member of Company management will meet with the suspect to gain his/her explanation of the situation. If it appears that a further in-depth investigation is required, the suspect employee will be placed on immediate suspension pending the outcome of the investigation. It will be made clear to the suspect employee that his/her employment is not being terminated and salary and benefits will continue. The employee will be instructed to call the Anti-Fraud Coordinator each morning at a specified time to ensure that the Company is aware of suspect's location during the course of the investigation. The following steps should be immediately taken:

- The suspect will be escorted to his/her desk by the Anti-fraud Coordinator and permitted to gather his/her personal effects. The employee must not be permitted to remove any MTL documents or equipment from his/her work area. The employee will be requested to surrender all keys and access cards for the duration of the suspension. The receptionists, Human Resources Department, and the Facilities Management will be notified that the subject is not permitted to enter the Company’s offices for the duration of the investigation. The employee will be instructed not to return to the Company offices unless specifically told to do so by the Anti-Fraud Coordinator or a member of the Company’s senior management. The employee should be told not to attempt to contact any other MTL employee during the course of the suspension.

- The suspect employee should be escorted out of the building by the Anti-Fraud Coordinator or a member of management. At no time during the interview and physical removal process should the employee be left unobserved. This is to prevent the destruction of evidence by the suspect.

- Any Company documents, assets, or computers in the suspect employee's possession but located outside of the Company premises should be immediately recovered. The recovery of such items should be done by the Anti-Fraud Coordinator accompanied by the suspect employee and one other member of the Company's management.

- The suspect's office, desk, files, and computer will be immediately secured. Other employees should not be allowed access to any evidence that could prove useful during the investigation.

Until the completion of the investigation, employees will be instructed not to contact or speak to the suspect. Information regarding the progress of the investigation should only be shared with employees or outsiders who have a legitimate need to know.

If the investigation reveals a probable fraud, a comprehensive review of the suspect's complete operational activities will take place to discover undetected frauds and possible collusion with other employees or outsiders. The suspect should once again be permitted to explain his/her actions and the events of the alleged fraud. Selected evidence will be presented to the suspect when appropriate to elicit responses and further explanations.

If the suspect confesses to fraud, a witnessed, hand-written statement detailing the fraud should be obtained from the suspect. Management should consider termination of employment if the commitment of fraud is established. No termination action will be taken without a comprehensive review by the Company's internal legal and Human Resources Departments.

The appropriate enforcement agencies and regulatory bodies may be contacted as needed and as required. The Company shall cooperate with law enforcement in the prosecution of all insurance fraud cases. If the loss is quantifiable, the Anti-Fraud Coordinator should consider filing a claim with the Company's fidelity insurance carrier and consider taking whatever civil action deemed appropriate to obtain restitution.

The Anti-Fraud Coordinator will also notify the appropriate law or regulatory enforcement body, in writing if required and as needed, that a fraud has occurred and take whatever legal action is necessary.

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:

- Providing training sessions on ethical practices and fraud awareness
- Producing and distributing the Guide to Business Practices and the Anti-Fraud Handbook
- Performing 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. MTL files such Annual Reports as required addressing fraud activity, policies and procedures.

Training

The Company conducts fraud training on an as needed basis at departmental and divisional meetings. Employees will be trained to recognize fraud indicators and the process for reporting them to the Anti-Fraud Coordinator. During these training sessions there are discussions of insurance fraud and occasionally outside experts are brought in to teach antifraud techniques. Real life examples from within the Company as well as training scenarios are presented.

Section VIII - Key Contacts

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

In person, by mail, by telephone:

Mailing Address:

MTL Insurance Company
1200 Jorie Boulevard
Oak Brook, IL 60523

Main Telephone Number:

630-990-1000

Contact:

Anti-Fraud Coordinator
Deputy General Counsel
General Counsel

Corporate Website:

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

SINCE 1904
MUTUAL TRUST
FINANCIAL GROUP®