Anti-Fraud Plan

A GUIDE

Fraud Awareness, Detection & Prevention
Introduction

Preventing fraud within the Company and by persons with which the Company does business is of utmost concern to senior management and represents one the Company’s highest priorities. Whether the Company is successful in its prevention techniques may have a direct impact on its continued success.

Attached is the Anti-Fraud Plan adopted by the Company to combat the increasing incidence of fraud in the insurance industry. This plan is intended to alert employees of the occurrence of fraud and to inform them of the procedures that should be followed if they become aware of suspicious or potentially fraudulent activities. The Company believes that an educated and informed team of employee is the most important step in addressing what is becoming one of the most serious threats to participants in the insurance industry.

The plan is divided into the following four sections:

Part 1—Fraud Defined
Part 2—Internal Fraud
Part 3—External Fraud
Part 4—Investigating and Reporting Fraud

Anti-Fraud Mission Statement

The mission of the anti-fraud plan is to prevent, detect, and report fraud by employees or company representatives, providers and other outside parties. Further, this plan encourages recommendations to management for changes in procedures and internal controls that would strengthen the Company’s ability to prevent and detect fraud against the Company.
Part 1—Fraud Defined

Fraud, according to the National Health Care Anti-Fraud Association, is defined as “the intentional deception or misrepresentation that the individual or entity makes knowing that the misrepresentation could result in some undue benefit to the individual, or the entity or to some other party.”

Experts, including the United States General Accounting Office, estimate that fraud, especially in the health-care field, totals approximately 10% of all benefits paid. The 1997 estimated national health care expense in the US is $1 trillion dollars; therefore, using these estimates, $100 billion of health care cost could be attributed to fraud.

Undetected fraud directly affects policyholders by way of higher premiums. It also affects insurance companies (and thus the number of people employed by those companies) if the cost of fraud cannot be minimized. Insurance companies must pass to policyholders such cost; in turn, policyholders may then search for companies with lower premiums.

Fraud is Criminal

Most fraudulent activities are considered to be criminal; however, the classification of fraudulent acts may vary from state to state. Some states have enacted (or are currently enacting) tougher laws to prosecute fraud offenders and to deter and prevent insurance fraud.

Types of Fraud

Fraud falls broadly into two categories.

Internal fraud is perpetrated against a company or its policyholders by agents, managers, or employees. Internal fraud includes, but is not limited to, the theft of company property or information, diversion of policyholder or company funds by employees, or intentional misrepresentation by agents about the characteristics of an insurance product.

External fraud, on the other hand, is directed against a company by individuals or entities, including, but not limited to: medical providers, policyholders, beneficiaries, vendors, and career criminals. The most common forms of external fraud consist of fraudulent claims and the negotiation of counterfeit checks.
Part 2—Internal Fraud

The two most common types of internal fraud are Agent and Employee Fraud.

Agent Fraud

A facet of the insurance industry, which has received much attention, is the various incidences of agent fraud (e.g., agent not remitting policyowners’ premiums to the insurer, agent making false claims of insurance products or future values, etc.). Many of the widely publicized cases involved well-known insurance companies who were required to pay millions of dollars in fines and restitution.

The Company has communicated to agents, where applicable, that agent fraud will not be tolerated. For instance, the General Agent’s Contract states that for various wrong acts (e.g., violating federal and state laws and regulations, wrongfully withholding funds belonging to any applicant, the unwarranted inducement to terminate a policy, etc.), the agent will not be paid commissions and lose any vested interest in policies. Also, agents are advised that, in circumstances where appropriate, the company will pursue a claim against an agent for misrepresentation or fraud. Further, agents have been informed that most Errors and Omissions policies contain an exclusion for acts committed with dishonest or fraudulent intent; therefore, the agent will be personally responsible for any fines or restitution.

Agent accounts are closely monitored and periodically audited to ensure that the agent is properly accounting for financial transactions with the Company. Employees are instructed to advise their supervisors of any irregularities in an agent’s account. If any irregularities are discovered, the agent will be asked to immediately respond and provide supporting documentation.

The Company will terminate the appointment of any agent who has exhibited an established a pattern of late remittance of premiums, who is unable to explain any financial irregularities, or who, based on its investigation of a claim or claims arising out of a pattern of activity on behalf of an agent, has knowingly misrepresented information on an application. Under certain circumstances, the Company may report the activity to the state insurance licensing authorities.

Employee Fraud (and Theft)

One of the company’s primary goals is to protect its property. Management makes it clear to employees that certain actions will not be tolerated. Management believes that one of the best loss prevention techniques is day-to-day contact by all managers with their employees. Managers are instructed to instill loyalty and foster high morale in their respective divisions through such contact and regularly scheduled staff meetings. Management believes that encouraging a “hands on” management style and open communication between management and employees can reduce the incidence of fraud and theft by employees.
Controls to Prevent Employee Fraud

General Controls-- The Company focuses on preventing fraud by establishing a good system of internal controls. General controls include, but are not limited to, the following:

• The Company maintains competent and trustworthy personnel with clear lines of authority and responsibility. Where appropriate, employees and officers are bonded.

• The Internal Audit department (and claims auditors, where appropriate) performs independent checks and verification of the internal controls associated with the claim and accounting departments to ensure that controls are adequate. If deemed appropriate, new controls are recommended.

Financial Controls—The Company has instituted financial controls, which it believes are crucial to avoiding fraud and embezzlement. In addition to supervisory review and close monitoring of employees handling funds, the Company has adopted the following prevention techniques.

• A sufficient segregation of duties within the Claims department and between the Claims department and other company departments. For example, claims personnel are not allowed to obtain possession of the physical benefit checks that they approved. All checks are prepared for mailing and mailed by the accounting department.

• Numerous systems edits that 1.) Disallow certain transactions for certain users, 2.) Disallow pre-designated combinations of transactions, and/or 3.) Produce reports that identify questionable transactions.

• Benefit approval procedures exist whereby pre-established procedures must be performed before a claim is paid. Such procedures include, but are not limited to, check approval authority based on the claims examiner’s experience and job position. If a claim benefit amount exceeds an examiner’s pre-authorized authority level, it is referred to the department supervisor/manager for review and approval prior to payment.

Computer Crime—To ensure that employees do not use computers to engage in unlawful activity, the following steps are taken by the Company:

• Periodic auditing of the computer system is conducted. Billings, payment of claims, policyholder identification, and related accounts are audited to ensure their integrity.

• Access to the computer and the computer process area is limited. Persons with access to the computer are assigned passwords and are instructed to keep their passwords stored in a secured place and not left out next to the computer. Access to the computers will be limited to those who need such access and confidential information will not be accessible through the general computer system.

• Procedural safeguards have been instituted so that no one person is responsible for all aspects of a financial transaction.

• All suspicious behavior is promptly investigated. Employees are instructed to immediately report any suspicious behavior and accounting or other irregularities to their supervisors.

Code of Ethics—The Company has adopted a Code of Ethics to which all employees are expected to adhere. All employees receive a copy of the Code and advised that they are expected to abide by the standards contained therein. Employees who violate the Code are disciplined. (See Attachment a — Employee Code of Ethics)
Part 3—External Fraud

Although there are similarities among all types of fraud, there are indicators of possible fraud distinct to health and life and accident insurance. Given the number of health claims paid greatly exceeds the number of life and accident claims, there is more information about health care fraud prevention available; therefore, it will be discussed first.

Since many aspects of health care fraud also apply to accident and life policies, it is beneficial for persons who administer life and accident policies to also review the health care information.

Health Care Fraud

External Health Care Fraud consists of “claimant fraud” and “provider fraud”. Claimant fraud is initiated by a claimant in order to obtain undue benefits from the insurance company. The most common type of claimant fraud involves falsifying or altering of claim documents.

Provider fraud is aggressively addressed by the National Health Care Anti-Fraud Association (NHCAA), who states that the variety of fraudulent reimbursement and billing practices in the health care area is potentially infinite. The most common fraudulent acts include, but are not limited to:

1. Billing for services, procedures and/or supplies that were not provided.
2. The intentional misrepresentation of any of the following for purposes of manipulating the benefits payable:
   a. The nature of services, procedures and/or supplies provided;
   b. The dates on which the services and/or treatments were rendered;
   c. The medical record of service and/or treatment provided;
   d. The condition treated or diagnosis made;
   e. The charges or reimbursement for services, procedures, and/or supplies provided;
   f. The identity of the provider or the recipient of services, procedures and/or supplies.
3. The deliberate performance of unwarranted/non-medically necessary services for the purpose of financial gain.

Such falsifications of claims involve the falsifying of patients’ symptoms and/or diagnoses and records of treatment. As such, they represent, at best, the creation of false medical histories for their patients. These undue benefits are used to determine the policyholder’s maximum annual or lifetime amounts and may result in a denial of a future valid claim. At worst, depending on the nature of the fraud, some providers place patients at physical risk solely for the purpose of generating claims.
Potential Fraud Indicators (also known as “Red Flags”)—both Claimant and Provider Fraud are described in the following section.

Claimant Fraud Indicators

While claims (and, where appropriate, underwriting) personnel are advised to watch for these signs, employees are advised to avoid prematurely labeling a claim as fraudulent or apparently legitimate. A claims processor or adjuster is instructed to point out discrepancies, but instructed to wait until an initial inquiry has been completed prior to offering his or her opinion.

• Losses claimed a short time after policy inception or shortly after a request for an increase in coverage.
• Contact with agent or broker that indicates the insured asked many hypothetical coverage questions prior to the purchase of the policy.
• “Black cloud” loss history, meaning the insured has had many prior losses
• The “perfect claim”, meaning the claimant provides receipts for all of the items claimed or the overly helpful claimants. Each may, without request, supply more information (proof) than necessary
• The insured is having personal or business related financial problems.
• Inducements offered to pay the claim
• Pressure from a claimant for a quick claim decision or payment. This may be evidenced by frequent and insistent telephone calls for claim payment or by the claimant's threatened use of an attorney and/or submission to the State Insurance Department.
• Claimant indicates an exceptional knowledge of medical procedures, claims processing, or insurance terminology.
• Claimants who hand deliver claim submissions or insist on picking up checks or claim drafts, rather than having them mailed. These actions may be an attempt to avoid further prosecution for mail fraud.
• Anonymous telephone calls inquiring about the status of a pending claim.
• The claimant refuses to provide, or cannot recall, answers to key details related to loss or associated with the services received.
• The claimant or the attorney is willing to accept less than the actual amount of the claim just to “help the company out” and to resolve the matter quickly.
• Frequent changes in address or returned mail marked “address unknown”

Additional “red flags” are listed below for specific portions of the health claim process, including the billings, receipts, and claim forms.

Billings
• Alteration of bills such as the dates, charges, diagnoses, and descriptions of services rendered. The correct information may have been changed (e.g., whited out, gone over in a different colored ink, etc.) to make the service eligible. Charges may also have been incurred prior to the effective date or subsequent to the termination date of the claimant’s coverage, prompting alteration.
• Photocopied bills, particularly those where the typed portion is clearer than the letterhead of preprinted items.
• Bills with irregular columns or bills that are not itemized.
• Typed or handwritten hospital bills.
• Fabricated bills, include
  1. Handwriting similarities by the claimant and provider
  2. Series of charges out of date sequence on the claim form.
  3. Mixture of typed and handwritten charges.
• Unassigned bills that are normally assigned (e.g., such as large hospital or surgery bills). Also, large bills that are marked “paid” in handwriting similar to that of the insured.
• Unusually low or high charges for routine services.
• Excessive drug expenses without associated provider charges.
• Bills containing charges for excessive treatment or procedures not normally associated with the stated diagnosis.

Receipts
• Drug receipts from the same pharmacy, but appear different (e.g., color, font)
• Prescriptions consecutively numbered although purchased on different dates
• Drug receipts cut off just below the total figure. This may be an indicator of an attempt to hide discounts.
• Duplicate receipts number appearing with new dates of service.

Claim Forms
• Signatures, handwritten, and/or typewritten entries in the Claimant’s and Provider’s sections of the claim forms that appear to be similar (i.e., used the same pen or typewriter)
• Misspelled medical or technical terms in the provider’s section of the form.
• Hospital “balance due” statements may be altered so that it appears charges were for a separate claim.
• Absence of the provider’s medical degree (i.e., “Dr. John Doe” instead of “John Doe, MD.”)
• Lack of the provider’s (rubber stamp) signature on the claim form
• Medical care visits on weekends or holidays.
• Overlapping dates of treatment with more than one physician
• A provider’s address which is not in the same geographic area as the claimant.
• Several claimants using the same physician or attorney.
• Excessive or vague documentation. Be suspicious if a claim form is the only information received, since it is easy to falsify a claim form.
• The claim submission is unusually late.
• The claimant fails to sign the medical information release authorization or answer key questions on the claim form.
Provider Fraud Indicators

Unscrupulous providers are constantly devising new schemes to defraud the health care insurance industry. Scams are growing dramatically bigger, bolder, and more sophisticated. There are, however, common characteristics of claim submission that may indicate potential provider fraud. These include:

- Insured’s address is the same as the provider’s address.
- Charges submitted for payment for which there is no supporting documentation available (e.g., x-rays, lab tests).
- Series of charges are out of date sequence on a claim form.
- Pattern of submitting assigned claims late.

The following indicators may surface from conversations with the provider, claimant, or other interested party.

- Unqualified individuals posing as licensed providers. Licensed providers can be verified by checking with the appropriate licensing agency.
- Advertisements of coinsurance forgiveness or discounts by providers. This is illegal in some states.
- Promotion of quack cures.

The following indicators are usually identified by complaints received from claimants when they review their Explanation of Benefits.

- Bills are submitted for canceled or missed appointments.
- Services charged for, but not rendered (fabricated services).
- Alterations of fees on bills that have been submitted for payment by the provider.

The potential for fraud may also be indicated by the actions of some providers. Please remember that providers are familiar with medical terminology and insurance procedures so provider fraud may be more difficult to identify than fraud by individual claimants. Provider fraud may be detected by reviewing the following:

- A pattern of submitting incorrect billings for which the provider routinely blames the billing clerk, secretary, or recently hired person.
- Assertive providers that demand immediate claim payment with special handling.
- Attending physicians that provide only a summary of treatment when actual records are requested.
- Provider that give inaccurate or incomplete patient histories.
- Improper coding, including:
  1. “Up-coding” or billing for excessive treatments --occurs when the provider lists a more serious diagnosis or procedure so that the reimbursement for services fall within the Medicare or provider’s reimbursement schedule.
  2. “Unbundling”—occurs when providers bill separately for services which are normally grouped together and for which there is a set reimbursement rate set by the insurer or by Medicare.
Life and Accident Insurance Fraud

Given that most life and accident policies issued by the Company are for benefit amounts that do not require extensive underwriting, most fraud indicators will surface when a claim for benefits is submitted.

To combat fraud, the examiners for Life and Accident policies closely examine claims submitted within the 2-year contestable period for information on the application that contains materially misleading information that is found to be relevant to the claim.

The following is a list of additional potential fraud indicators:

- Beneficiary files a claim using *suspicious* documentation
- Claimant is found to possess multiple policies, which name beneficiaries with questionable insurable interest.
- Death allegedly occurs on foreign soil and proof of death and/or proper identification of decedent is suspicious.
- Death occurs shortly after decedent purchases a large policy or request increases to existing policies.
- Pressures from a claimant for a quick decision or payment via frequent and insistent telephone calls demanding claim payment during our investigation process and threats of filing complaints with the State Insurance Department, public media, etc.
- Lack of cooperation on the part of a claimant beneficiary or in executing or furnishing an authorization for release of medical and/or relevant records and furnishing information requested by the Company.
- Inducements offered to pay the claim of settle for less than the amount stated in the policy.
- Mysterious disappearance of insured where investigation reveals that the insured had financial or criminal problems prior to disappearance.
Part 4—Investigating and Reporting Fraud

Special Investigative Unit

The Company has assembled a Special Investigative Unit (SIU) comprising of the following persons:

(See Attachment B – Special Investigative Unit)

Although members of the SIU frequently use the expertise of all managers, especially Claim Examiners and Underwriters, the appointment of the SIU members was made so that independence exists between the SIU and claims and underwriting units.

Other Investigative Personnel

Claim examiners, underwriters, and customer service representatives are the first lines of defense of external fraud. Therefore, in the routine investigations conducted by such personnel, it is important that they make early determinations of potential fraudulent activity and referred such to their unit manager.

The Company uses a variety of individuals to aid in identifying fraud. These individuals include Claims (described in detail later in this section), New Business, Internal Audit, and Legal personnel, as well as outside individuals, when necessary. The following are the most common ways suspected fraud is identified:

• Referrals from policyholders that a claim or application may be fraudulent.
• Specifically designed reports generated by Data Processing that identify known patterns of potential fraud.
• An individual employed as a full-time claims auditor who analyzes documents and reports that were designed to expose potential fraud.
• The claim personnel who conducts surprise rotating audits for all type of claims transactions
• Review of applications at new business for unusual or suspicious items.

Once external fraud is identified or suspected, the matter should be promptly reported to the employee's manager. An initial investigation of the matter is conducted. If there is merit to the suspicion, details of the matter should be promptly referred to a member of the Special Investigative Unit by the department manager.

Although the reports listed above are used identify external fraud, internal fraud can also be identified by other employees, agent, and company officers. To aid in the identification of internal fraud, the Company maintains an “open door policy” whereby employees can voice their concerns regarding the work or working environment and/or conditions. Employees are encouraged to discuss any concerns with their supervisor and/or manager, the personnel department, or any other manager or officer of the Company. Note that employees have also been informed that they can also report any concerns anonymously.
Investigation by Claims Department

Although, claims examiners (and claims management) are qualified to investigate suspected fraudulent claims, all suspected claims should be communicated to department management prior to engaging in an inquiry. An inquiry file should be maintained that shows the information gather and results. This file will be forwarded to department management and later to the SIU.

The following information should be obtained and/or assessed by claims personnel in connection with the investigation of a suspected fraudulent claim, if deemed appropriate.

Claimant
- Statement (outlining the claimant’s knowledge),
- General reputation and character,
- The financial condition of the claimant, as determined through an inspection of books and other records if where possible,
- General living conditions,
- Claimant’s hobbies and sports,
- Social activities of the claimant and his/her level of involvement,
- Claimant’s history, including all previous residences, employers, and businesses,
- Any information about suspicious, mysterious, or illegal about the claimant’s business or employment. (The reputation of the business may be checked with the Better Business Bureau and/or trade associations. Police records may be reviewed to confirm this information, where possible.)

Previous Claims
- Insurance, particularly life and accident and health policies should be checked with current and past insurers to determine the past claim record of the claimant.
- Claims reporting bureaus are checked to review reports pertaining not only to the claimant, but also regarding any suspicious indications concerning doctors, lawyers, and even witnesses.

Medical Information
- Reputation and/or qualification of attending doctors and other professionals,
- Thorough medical examination by a qualified specialist (if possible),
- Hospital records,
- New x-ray reports, scans, and laboratory tests (if deemed necessary),
- Medical expenses
  1. Attending doctors, specialists, and dentists bills,
  2. Registered and practical nurses’ fees,
  3. Hospital and clinic bills,
  4. Ambulance charges,
  5. X-rays, special medical equipment and laboratory charges,
  6. Prosthetic appliances or surgical apparatus,
  7. Medicines, drugs, and other pharmaceutical supplies.
Witness Interviews

- Claims personnel may contact the witnesses and other person with information relevant to the claim. All details of the transaction of occurrence are to be covered. A statement should document the topics discussed. Personnel are advised to not challenge witness’s recollection or bring to his or her attention conflicts in testimony.
- In appropriate cases, employers may be instructed to investigate the witness’s background and claims activity.

Agent Interview

- The agent who sold the policy may be asked questions related to the claim, including how the policy was sold and details of the communications between the agent and the insured.

Please keep in mind that if the above information cannot be obtained within a reasonable amount of time, employees should refer the information to management to ensure the time limit requirements, that are unique to each state, can be met.

Conclusion of Investigation, Referral to SIU

Once sufficient information is obtained to substantiate their suspicions of fraud, claims personnel should present the facts of the case to their manager. Upon determining that the facts in the case warrant a fraud investigation, unit managers and their respective Vice Presidents are authorized to refer suspected fraud to the SIU for investigation. The SIU, as an independent unit, is primarily responsible for investigating suspected fraud.

The “criteria” for determining whether a case should be referred to the SIU is based on the definition of “fraud”. In general, fraud is considered to exist where the perpetrator knowingly, and with intent, defrauded (or attempted to defraud) the Company.

In submitting evidence of suspected fraud, employees and managers should keep the following points in mind:

- The report should accurate and truthful.
- The investigation file must reflect a complete and balanced inquiry. Employees are instructed to avoid derogatory or inflammatory remarks about anyone and avoid prejudging the legitimacy of the claim.
- Employees are instructed to use phrases such as “conflict in evidence”, “no record of purchase”, “there are some discrepancies”, or “serious questions have been raised concerning this claim” so that the facts and evidence may speak for themselves.
- Employees are advised to avoid documenting internal or office disagreements, in other words, avoid “finger pointing” regarding the handling or investigation of the claim. Such items shall be referred to department managers for handling.

It should be stated on the claim routing sheet or memo that the claim is being referred to Counsel or the SIU “in anticipation of litigation”.

Page 13

10-3-07
SIU Investigation

Items referred to the SIU for fraud investigation are diverse in nature. Therefore, much of the investigation work completed by the investigators will be tailored toward obtaining sufficient information to render a decision as to whether fraud exists. Nevertheless, the investigator (working with legal to ensure that the Company's rights can be preserved) will usually complete the following steps when investigating fraud:

- Carefully review all information. This includes obtaining and closely reviewing copies (or originals, if necessary and possible) of the policy files.
- If an employee of the company has had contact with key persons in the investigation, then the investigator should interview the employee to ensure that all facts of any contact have been sufficiently documented in the case file.
- If dates are an important factor in the case, the investigator should construct a timeline of events.
- If the facts of the case require external confirmation of facts, the investigator should work with legal to develop the most appropriate method to obtain the information. For instance, if a claim received from the provider appears to be fraudulent, then a confirmation of the service date and procedures with the policyholder might be necessary. This letter should be worded so that if the case were civil or criminal charges that it would present the strongest case.

Decision from Counsel and/or Special Investigative Unit

Once the SIU investigator obtains sufficient information to render an opinion, the information shall be discussed with management, Counsel, and the Head of the SIU. If it is decided that the matter will be considered fraud, a person will be designated to report the incidence to the respective external agency (or agencies) and will serve as the contact person for the case. This person is responsible for keeping members of the SIU aware of the progress on the case. This procedure will also help to prevent multiple reporting to external agencies and allow the company to receive the information in one location.

If the Company, who in good faith, has cause to believe that insurance fraud has been or is being committed, the Company shall report the suspected fraud to the:

1. State’s fraud division or Department of Insurance (or their respective designees); and/or
2. Local, state, or federal authorities or agencies.

Individual states have different reporting requirements, such as time frame and method of communication (e.g., the State of New York requires that their Insurance Frauds Bureau be notified on a prescribed form within 30 days of discovery). If the reporting requirements are not known, personnel should request the aid of the legal department.

Please note that reporting immunity for suspected fraud also varies by state. In an effort to protect certain privileges available to the Company (especially for states with no reporting immunity), consideration will be given to verbally reporting suspected fraud to law enforcement and appropriate prosecutor's offices. At that time the Company’s
representative will ask that they request in writing a copy of the investigator's current report.

In short, by involving the legal department in the reporting process prior to releasing the information to external agencies, the Company will be better able to protect itself from the risks associated with some state's lack of immunity statutes.

**Cooperation with Law Enforcement Authorities**

After the case is submitted to the respective law enforcement agency for possible criminal prosecution, the Company and its employees will cooperate with prosecutors and law enforcement officials.

**Civil Action Against Fraudulent Activity**

If an item is determined to be fraudulent, Counsel will seek collection of restitution of financial loss caused by the fraud. If the perpetrator of the fraud is tried and convicted, the Company will seek restitution through criminal proceedings. If there is no criminal action, the Company will seek restitution in a civil action.

**Fraud Database**

All suspected fraud items shall be logged as a fraud item into the fraud database. The Company's determination as to whether the suspected fraud item has merit and the status of various enforcement agencies' action on a case will be noted on the system. This database shall also be used by the Special Investigative Unit to determine if trends exist with regard to fraud.

The Company's fraud "database" is located on the Internal Audit's Share Directory and is password protected. It is currently maintained using the Microsoft Excel® software on a LAN-based network (if the need arises in the future for more canned reports or for fixed data fields, the information may easily be transferred to a Microsoft Access® database). This network is backed up nightly and is adequately secured from users outside the network. The ability to update the database is limited to the SIU Investigative Staff.

Hard copies of the fraud files, including original signed witness statements or affidavits, are retained in the legal department pending further proceedings and/or submitting copies to the local, state, or federal investigative authorities.

The SIU shall use the information from the database to report to the audit committee and upper management on a periodic basis. The information will also be used to make annual reports to states that require fraud reports.