Minnesota

ANTI-FRAUD PLAN

PRUDENTIAL INSURANCE COMPANY of AMERICA
NAIC Group #304
NAIC # 68241

Prudential Annuity and Life Assurance Corporation
NAIC # 86630

Pruco Life Insurance Company
NAIC # 79227

Prudential Retirement Insurance and Annuity Company
NAIC # 93629

Table of Contents

I. Introduction

Pursuant to § 60A.954 of the Minnesota Statutes Annotated, the following is Prudential's revised Anti-Fraud Plan as maintained by the Corporate Investigations Division ("CID"). CID is responsible for investigating and reporting fraud associated with the various Prudential entities identified on the cover page of this document to the Minnesota Department of Commerce.

It is confirmed that designated executive, Marc Rothenberg, VP & Corporate Counsel, has reviewed and approved this plan.

a. Company Profile

Founded in 1875, Prudential Financial is headquartered in Newark, New Jersey. The Prudential Insurance Company of America ("PICA") is a multi-line insurance company offering individual life, annuities, retirement and group insurance products through distinct business divisions. The U.S. Individual Life and Group Insurance division conducts its business through the Individual Life and Group Insurance segments.

- Our Individual Life segment manufactures and distributes individual variable life, term life and universal life insurance products, primarily to the U.S. mass middle, mass affluent and affluent markets.

- Our Group Insurance segment manufactures and distributes a full range of group life, long-term and short-term group disability, and group corporate-owned, bank-owned and trust-owned life insurance in the U.S., primarily to institutional clients for use in connection with employee and membership benefits plans. Group Insurance also sells accidental death and dismemberment and other ancillary coverages, and provides plan administrative services in connection with its insurance coverages.

b. Fraud Prevention Policy and Controls

Prudential's Fraud Prevention Policy, which is reviewed annually, defines fraud "as any act characterized by deceit, concealment or violation of trust that is committed by an individual or organization to obtain money, property or services; avoid payment or loss of services; or secure a personal or business advantage." It provides in pertinent part:

> This Policy is intended to reduce the possibility of fraudulent conduct and to preserve the integrity of Prudential's business records. Prudential vigorously protects itself against potential acts of fraud, pursues those who perpetrate or attempt fraud against the Company and refers individuals for prosecution, where appropriate, to the extent allowed by local laws. This Policy covers known and suspected fraudulent acts committed internally by employees and/or external parties.

> Employees must report instances of known or suspected fraud. Employees are also prohibited from preparing false records or falsifying or inappropriately altering Prudential business records or directing others to do so. Under no circumstances may an employee offer to sign, actually sign, or direct others to sign, a document for or on behalf of a customer, policyholder, shareholder or applicant for any product, service or benefit offered by the Company. Employees are prohibited from knowingly accepting or processing forged, falsified or inappropriately altered records, instruments or documents.

The Fraud Prevention Policy requires employees to "promptly report instances of known or suspected fraud, and cooperate with any internal or external investigations relating thereto." Company employees "may report instances of known or suspected fraud directly to CID. Alternatively, employees may report instances of known or suspected fraud: (1) to their business or corporate department supervisors or managers, if appropriate under the circumstances, (2) to the Law, Compliance, Human Resources or Internal Audit Departments, or (3) to their local business ethics contacts, each of which must promptly notify CID."

Employees wishing anonymity may also make referrals to the Company's Ethics Hotline, a confidential resource for associates to ask questions, get advice, raise concerns, and clarify issues on a variety of subjects, including fraud.

In addition, Prudential is committed to the principle that all business should be conducted in a professional, fair and trustworthy manner and transacted in accordance with high standards of ethical conduct. All associates are expected to conduct business in a manner consistent with these principles to maintain the trust and respect of fellow employees, customers, business colleagues, and the general public.

In support of Prudential's efforts to mitigate fraud, Prudential has established numerous internal controls to reduce the opportunity for fraud, including:

- Restricting access to computer systems.
- Identifying the origin of transactions and requiring frequent changes of confidential passwords for access to internal systems.
- Using generally accepted accounting practices that separate cash and financial instrument handling from reporting.
- Using system-wide requirements for processing disbursements.
- Providing training on potential red flags or characteristics of suspected fraudulent activity.
- Using automated systems to verify information provided during the underwriting and application phase.
- Maintaining an internal auditing staff to search for and identify weaknesses in existing controls.

II. Corporate Investigations Division

Pursuant to Prudential's Fraud Prevention Policy, "CID has oversight responsibility for all fraud investigations conducted enterprise-wide and, within the U.S., for related regulatory reporting." CID has experienced full-time staff members whose primary responsibilities include investigating and reporting fraud across all product lines. CID is an independent function and sits within Prudential's Law, Compliance, Business Ethics and External Affairs Department ("LCBE").

In the first quarter of 2017, the Individual Life Insurance Special Investigations Unit ("ILI SIU"), which had been responsible for pre-issuance and claims investigations for the Company's Individual Life Insurance business, integrated into CID and no longer exists within the Individual Life Insurance business. This plan reflects the post-integration structure of CID.

a. Mission

Prudential views insurance fraud as a serious crime and works vigorously to detect and pursue acts of fraud and those who perpetrate them. As such, CID's mission statement is:

> "To detect, prevent and investigate activities that threaten Prudential and its customers."

b. Responsibilities:

CID is responsible, among other things, for:

- Conducting investigations related to suspected fraudulent activity by internal or external persons or entities.
- Managing, directing and coordinating case referrals from the different businesses.
- Reporting investigative findings to relevant business stakeholders, including the risk, compliance, and legal functions.
- When required, reporting to state Departments of Insurance ("DOIs"), state Departments of Aging (or their equivalent), regulatory agencies, and law enforcement.
- Analyzing data from a centralized fraud reporting and case management database to provide risk assessment and trending of fraudulent activity.
- Assessing risk and working with businesses and centralized business functions to mitigate risk.
- Developing and delivering training to integral anti-fraud personnel on issues relating to, among other things, the Company's Fraud Prevention Policy, red flag indicators of suspected fraudulent activity, and reporting of these activities to CID for investigation.

c. Composition

CID reports to the Chief Litigation Officer, Eric Schwimmer, and is co-led by Marc Rothenberg, VP & Corporate Counsel, and Susanna Gray, VP & Corporate Counsel. Mr. Rothenberg holds a Juris Doctor degree and has over 20 years of complex criminal enforcement, investigation and litigation experience as a Federal Prosecutor, government enforcement attorney, and Partner in the White Collar Defense and Investigations Practice Group of an Am Law 100 firm representing corporations and individuals in financial crimes enforcement actions. Ms. Gray holds a joint Juris Doctor/Masters in Criminal Justice degree and has over 15 years of investigations and litigation experience as an in-house counsel, Senior Litigation Associate in an Am Law 100 firm, and federal law clerk.

CID's members consist of 43 associates:

- Vice Presidents (3)
- Directors (3)
- Managers (3)
- Senior Investigators (4)
- Investigators (20)
- Associate Investigators (5)
- Senior Investigative Associate (1)
- Operations Analyst (1)
- Associate Operations Analyst (1)
- Paralegal (1)
- Executive Assistant (1)

Each investigator has the required knowledge, education, training and experience to conduct effective investigations, as well as knowledge of insurance and related laws and the use of investigative database resources. CID's collective experience includes law enforcement, financial services, regulatory, compliance, and risk management. In addition, some members have advanced degrees (i.e., JD, MBA, MCJ, etc.) and are Certified Fraud Examiners. CID's current organizational structure is attached as Exhibit A.

Within CID, Marc Rothenberg, VP & Corporate Counsel, is the designated executive and primary contact person.

Marc Rothenberg
Vice President and Corporate Counsel
Corporate Investigations Division
The Prudential Insurance Company of America
213 Washington Street
Newark, NJ 07102
973-802-7603
973-802-2784 (Fax)
marc.rothenberg@prudential.com

d. Associations and Memberships

Employees within CID participate in professional organizations committed to anti-fraud activities and actively seek training through such organizations, including:

- Coalition Against Insurance Fraud (CAIF)
- New York Alliance Against Insurance Fraud (NYAAIF)
- International Association of Financial Crimes Investigators (IAFCI)
- International Association of Special Investigation Units (IASIU), as well as local chapters
- Association of Certified Fraud Examiners (CFE)
- The Association of Investigative Managers (AIM)
- Life and Health International Claim Association (ICA)
- Midwest Insurance Fraud Prevention Association (MIFPA)

e. Policies and Procedures

CID has established policies and procedures to ensure that allegations of fraudulent activity are thoroughly investigated and resolved, including reporting to state DOIs and outside regulatory and law enforcement agencies when appropriate (see Section V).

CID maintains Standard Operating Procedures ("SOPs") in a corporate database available to all employees in the division. The SOPs cover, among other things, investigator responsibilities, organizational structure of the division, state fraud reporting requirements, and guidelines for conducting interviews and investigations.

CID's SOPs for conducting investigations include specific protocols designed to ensure that all investigations are conducted within a framework that results in objective findings, based upon the evidence and reasonable inferences. Investigators review the details and facts of the case intake referral, including any documents attached to the referral, as well as any applicable Company policies or standards. A written investigative plan is then completed within a reasonable period following the investigator's review and is maintained in the CID document management system. The plan is updated during the course of the investigation as needed based upon facts ascertained, as well as any change in the risk profile.

During the course of the investigation, the investigator will perform record checks, conduct interviews, and collect and analyze evidence. When the investigation is complete, the investigator details the investigative findings in a closing document. This document describes the alleged misconduct, summarizes the facts and findings and the conclusions reached. Investigations are generally conducted under a preponderance of evidence standard based upon reasonable determinations of the evidence and inferences drawn from the same. A heightened standard may be utilized as appropriate, including pursuant to legal or regulatory requirements. In such instances, the standard will be noted.

These SOPs also cover evidence collection and storage, including maintaining chain of custody, as well as file and evidence retention so that evidence is preserved and can be produced to state DOIs, law enforcement and regulators.

f. Comprehensive Databases

CID subscribes to the following databases as part of its anti-fraud program:

LexisNexis Accurint: Provides comprehensive public and proprietary records information, including personal identifiers, business records, professional licenses, nationwide bankruptcy, criminal and civil litigation records, liens and judgments, property records, etc.

LexisNexis IRS Verify: Provides 4506T form fulfillment services, automated and guided ordering capabilities, advanced quality screening, delivery of key financial data in a summarized format, and centralized access to support single users or multiple branches. With a properly executed 4506T form, CID can request and retrieve IRS records for the subjects of its investigations.

Thomson Reuters CLEAR: An online investigative platform designed specifically to meet the needs of investigators. Like Accurint, the database provides a vast collection of public and proprietary records. It also provides additional Internet search capabilities via its Web Analytics feature.

Clear Investigative Advantage: Provides background screening services, including searches for county, state and federal criminal records.

Dun and Bradstreet: Provides domestic and international company reports, which include corporate history and registration details, business affiliations, key executives, financials, etc.

Examination Management Services, Inc.: An RX profile system, which provides a comprehensive list of prescriptions for insured individuals obtained from various prescription drug plans.

Public Access to Court Electronic Records (PACER): An electronic public access service that allows users to obtain case and docket information online from federal appellate, district, and bankruptcy courts. PACER is provided by the Federal Judiciary in keeping with its commitment to providing public access to court information via a centralized service.

RegEd: A provider of Compliance Management, Compliance Education and Licensing and Registration solutions and services to broker-dealers, insurance carriers and insurance distributors. Its database is primarily used for broker due diligence.

Search Systems: A directory of links to public record databases and online services on the Internet.

III. Procedures for Detecting Fraud and Referring to CID

Detection of suspected instances of insurance fraud begins with Prudential's Anti-Fraud Training Program (Section IV). As set forth in the Anti-Fraud Training Program section, Prudential provides both new hire and annual continuing education fraud training to integral anti-fraud personnel. Integral anti-fraud personnel are employees whose duties may include processing, investigating, or litigating matters related to the payment or denial of a claim or application for adjudication or claim or application for insurance. Included within both the new hire and annual training are modules covering early detection of suspected insurance fraud.

CID maintains comprehensive lists of potential red flags of suspected insurance fraud, which are included in Prudential's Anti-Fraud Training Program, as well as disseminated to each individual business unit and incorporated into their SOPs. The red flags are set forth below in section III(a).

In addition, each business unit within Individual Life, Group, Annuities, and Retirement, including, but not limited to, underwriting, claims, and call centers, have specific procedures for the detection and reporting of suspected insurance fraud to CID for investigation. The procedures provide for comparison of the claim, application or transaction against red flags, patterns and trends of possible fraud and events or behavior of the person(s) submitting the transaction.

Prudential's claims and underwriting units also conduct monthly quality reviews to identify possible fraud red flags. In addition, periodic post-payment claim file reviews are conducted manually to ensure that suspected fraudulent claims are being identified and reported.

Individual Life Insurance utilizes a Data Verification Report ("DVR") system to help detect underwriting and application fraud. Database checks verify the identity of the customer by crosschecking various sources to validate names, addresses, dates of birth, telephone numbers and social security numbers. It also provides searches of the social security death index, criminal records and other public records, such as liens, judgments, bankruptcies and lawsuits.

Prudential also maintains a Field Office Examination Program, which requires the inspection of all Offices of Supervisory Jurisdiction ("OSJs") and non-OSJs. The inspection protocol scope includes such topics as supervision, licensing, registration and training, correspondence and communications with the public, marketing materials, handling of funds and control of customer accounts. The program includes reviews of client files, common address reports, oversight reports, and outside business activities, which aid in the identification and monitoring of potential inappropriate and/or fraudulent activities by producers.

Additionally, all disbursements are processed through an automated payment system called the Prudential Integrated Disbursement Environment ("PRIDE"). PRIDE has security in place to ensure payment requests are not approved by the same person. There is segregation

of duties implemented in all PRIDE access roles. Semi-annual security access reviews are also conducted in May and November.

Business units take intermediate steps prior to referring suspected instances of fraud to CID. In Annuities, Retirement and Individual Life Insurance, Anti-Fraud Coordinators review all cases prior to forwarding to CID in order to ensure the referrals are in good order. Anti-Fraud Coordinators also determine whether rights restrictions, alerts, or additional actions are to be taken on a contract. In Individual Life Insurance Claims, suspected fraud is reviewed by senior management prior to submission to CID. In Individual Life Insurance Underwriting, the Corporate Underwriters review prior to submission to CID. In Group Insurance, upon suspicion of a claim fraud, a claims manager or underwriter discusses the situation with his/her immediate supervisor (i.e., Team Lead, Associate Manager or Manager) to determine if the matter should be referred to CID. Law Department personnel may refer directly to CID.

Fraud complaints can also arise from whistleblowers, the public and policy holders. These complaints can be reported to Prudential in a number of ways. CID maintains both a Fraud Hotline and Fraud Mailbox that provide associates and the public the opportunity to report potential fraud to the Company. The Fraud Hotline phone number (1-877-362-9232) and e-mail (investigations@prudential.com) can be found on the Company's website, through a dedicated "Report Fraud" hotlink.

a. Fraud Red Flags/Indicators

i. Internal Fraud

Internal fraud may be perpetrated against the Company or its contract/policy owners by employees at all levels within the Company. Internal fraud may involve theft of proprietary information or company property, improper relationships with vendors or consultants involving conflicts of interest, diversion of contract/policy owner or Company funds by employees, use of confidential or proprietary information for personal gain by employees, or any other acts that may constitute an intentional deception against the Company for personal gain.

Internal fraud examples include:

- Intentionally miscalculating benefits and stealing the difference.
- Intentionally misstating financial results.
- Delaying benefit processing to improve reporting results.
- Forging or altering any document submitted by, or account belonging to, a client.
- Forging or altering a check, bank draft, or other financial document.
- Unauthorized use of another employee's ID or password.
- Accepting bribes or kickbacks in cash or in kind.
- Falsifying employee timesheets or other records, which determine employee benefits or compensation.
- Inflating/falsifying expense reports.

- Stealing furniture, personal computers, or other equipment or supplies owned or leased by the Company.
- Selling or giving away confidential or proprietary information.
- Seeking or accepting anything of material value from vendors or persons providing services/materials to the Company (exception: a perishable gift less than $100 per person, such as candy, flowers, an occasional dinner or a ticket to a sporting event or the theatre).
- Seeking or accepting anything of value from any employee in exchange for preferential treatment.

Certain red flags or warning signs may exist that could influence an employee to commit fraud, including:

- Financial pressure on the individual.
- Poor internal controls (e.g., the ability of one person to process transactions, issue checks and make accounting entries).

The following is a non-exclusive list of indicators related to internal fraud. The occurrence of a specific indicator, in and of itself, does not substantiate the existence of fraudulent acts, but rather should serve as a basis for raising suspicion and possible referral to CID.

- Operating fluctuations that cannot be explained.
- Large or unusual transactions, particularly at year-end, with a material effect on an area's budget or sales targets.
- Normal processing procedures overridden without adequate explanation.
- Accounting entries made without proper approval.

ii. External Fraud

External fraud is directed against the Company by contract/policy owners, beneficiaries, brokers/agents, vendors or other third parties. It typically involves an attempt to defraud the Company or one or more of its contract/policy owners. To defraud, for these purposes, is defined as "to make a misrepresentation of an existing material fact, knowing it to be false or making it recklessly without regard to whether it is true or false, intending one to rely and under circumstances in which such person does rely to his damage." Black's Law Dictionary (6th Ed. 1991). External fraud may involve such schemes as the forgery of documents used to withdraw funds from a contract/policy, fraudulent claims for death benefits, the use of Prudential insurance and annuity products to conceal the origin of illicit funds, the negotiation of counterfeit or forged checks, or any other acts that may constitute an intentional deception against the Company for personal gain.

External fraud examples include:

- Submitting altered or forged documents to the Company in order to withdraw or transfer/exchange funds.

- Submitting false claims.
- Negotiating counterfeit, altered or forged checks.
- Accepting bribes or kickbacks in cash or in kind.
- Stealing furniture, personal computers, or other equipment or supplies owned or leased by the Company.
- Selling or giving away confidential or proprietary information.
- Altering applications, forms or other documents submitted to the Company.
- Providing false or misleading illustrations.
- Failing to deliver money due to contract/policy owner, beneficiary or other person entitled to any sum payable by the Company.
- Failing to remit purchase payments or premiums to the Company in a timely manner.
- Collecting sums larger than the actual purchase payments or premiums for a policy/contract.
- Intentionally misrepresenting to customers, or prospective customers, the characteristics or future performance of Company products.

The following is a non-exclusive list of indicators related to external fraud. The occurrence of a specific indicator, in and of itself, does not substantiate the existence of fraudulent acts, but rather should serve as a basis for raising suspicion and possible referral to CID.

- Partial or full surrender request is received shortly after a change of address on the contract/policy.
- Partial or full surrender request indicates that funds should be sent to a location other than the address of record.
- Partial or full surrender request indicates the funds should be payable to an individual other than the owner(s), or directed to an account that is not of identical ownership.
- The address of record for one or more contracts with the same broker/agent is identical.
- The individual whose life determines payment of death benefits dies within two (2) years of the effective date of the insurance coverage.
- False and/or misleading information is discovered on the contract application, claim paperwork, surrender paperwork, or transfer/exchange paperwork.
- The claimant/requestor provides unusually detailed or unusually vague information and documentation.
- The claimant/requestor is apparently experiencing events that may lead to financial difficulty, such as separation or divorce, unemployment, business declines or defaults, or medical or legal expenses unrelated to the claim/requested transaction.
- Photocopies are submitted, rather than original documents, to support the claim or requested transaction.
- Submitted documents appear to be altered and/or forged.

The following is a non-exclusive list of specific indicators related to claims fraud. The occurrence of a specific indicator, in and of itself, does not substantiate the existence of fraudulent acts, but rather should serve as a basis for raising suspicion on the part of the Claims Examiner or Client Services Representative and possible referral to CID.

- The application contains misleading information that is relevant to the transaction request or claim.
- A beneficiary files a claim using suspicious documentation.
- An owner is found to possess multiple policies that name beneficiaries with a questionable insurable interest (for life insurance).
- Death allegedly occurs on foreign soil and proof of death and/or proper identification of decedent is suspicious.
- Death occurs under unusual or apparently criminal circumstances.
- Death of the insured occurs shortly after the owner purchases a contract/policy with a large death benefit or increases existing coverage amounts.
- Signature(s) on forms received does not match signature(s) already on file with the Company.
- Claims for subjective diagnoses - back pain, stress, nervous disorders, headaches, etc.
- Claimed length of disability seems excessive for the claimed diagnosis.
- Claimant is never available to take calls at the residence during normal business hours.
- Individuals who have difficulty keeping jobs.
- Information provided on the application or claim form develops to be false or incomplete, including telephone numbers, Social Security numbers, supervisor's name, employer's telephone, addresses, etc.

The following is a non-exclusive list of specific indicators related to broker/agent fraud. The occurrence of a specific indicator, in and of itself, does not substantiate the existence of fraudulent acts, but rather should serve as a basis for raising suspicion and possible referral to CID.

- The broker/agent is often behind in submitting applications and/or supporting documentation to the Company.
- The broker/agent fails to timely submit premiums or purchase payments to the Company.
- The broker/agent advises contract/policy owners to conduct all business directly with the broker/agent, and/or to refrain from contacting the Company directly.
- The broker/agent advises contract/policy owners to have all confirmations and quarterly statements sent to the broker/agent only.
- A sudden or unusual amount of activity (particularly full or partial surrenders) in contract/policy owner accounts that have the same broker/agent-of-record.
- The broker/agent asks for special treatment.
- The contract/policy owner has never heard of the broker/agent or of the Company.
- The Company receives an unusual number of complaints about a particular broker/agent.
- The broker/agent refuses to submit required documentation to the Company with appropriate contract/policy owner signatures, without adequate explanation.

IV. Anti-Fraud Training Program

a. CID Investigator Training

The members of CID receive basic entry level training, which is no less than nine (9) hours of classroom instruction. In addition, members of CID receive annual continuing education training of no less than nine (9) hours.

Basic entry level and continuing education training includes, among other topics, courses on fraud, red flag indicators of insurance fraud, elder financial exploitation, and applicable state fraud statutes. Training is also provided on available investigative resources (i.e., systems, products, internal and external databases).

For investigators holding a CFE designation, the Association of Certified Fraud Examiners requires twenty (20) hours of training to maintain certification. External training involves attending or viewing specific courses on investigative techniques and practices, as well as participation in various industry associations, seminars, and conferences.

CID members record both their internal and external training in an enterprise-wide database called Learning Connection. Web Based Training ("WBT") is also facilitated by this system, which automatically logs completion of WBT courses.

b. Associate Fraud Awareness Training

Prudential is committed to the prevention of insurance fraud. Providing fraud awareness training for all associates who work in roles that may encounter fraud is one of the first steps in fulfilling this commitment. Prudential has established and maintains an Anti-Fraud Training Program to develop and improve the fraud awareness of integral anti-fraud personnel.

i. Group Insurance

Within one hundred and eighty (180) days of employment, Prudential provides a minimum of four and one-half (4.5) hours of instructor led new hire fraud awareness training for its Group Insurance employees, as well as for its personnel who have responsibility for Long-Term Care Insurance ("LTC") and those who work in Centralized Business Services supporting Group Insurance Underwriting and Claims. In addition, these employees receive annual continuing education training of no less than two (2) hours.

The basic entry level training provides, among other things, (i) an overview of the procedures for detecting suspected insurance fraud; (ii) a comparison of insurance transactions against patterns or trends of possible fraud and red flags; (iii) a review of events or circumstances present on a claim, including the behavior or history of person submitting an application or claim; (iv) other criteria that may indicate possible fraud; and (v) case examples reviewing investigative steps and techniques. The training also includes information regarding the function and purpose of CID, an overview of fraud detection and referral of suspected

insurance fraud to CID for investigation, Prudential's Fraud Prevention Policy, and a review of insurance fraud reporting requirements.

ii. Other Business Units

Prudential's integral anti-fraud associates in businesses other than those set forth in (b)(i) receive anti-fraud orientation within ninety (90) days of employment via a general fraud awareness WBT course. The course includes information regarding the function and purpose of CID, overview of fraud detection and referral of suspected insurance fraud to CID, mandatory reporting requirements for various state DOIs, and CID organization and contact telephone numbers. The Company has also developed four additional WBT courses tailored to specific job responsibilities and product lines, such as Fraud Awareness for Individual Life Insurance, Group Insurance, Call Center, and Financial Professionals. Each WBT takes approximately one-half (0.5) hour to complete. In addition, these associates receive annual continuing education training of no less than one (1) hour.

Participant rosters and sign-in logs for all in-person fraud awareness training are maintained by CID. WBT training is facilitated by, and automatically logged in, Learning Connection.

V. Reporting of Insurance Fraud

In compliance with the Minnesota Statutes Annotated, all incidents of suspected insurance fraud as defined by § 60A.951 will be reported to the Minnesota Department of Commerce, as well as appropriate law enforcement and other regulatory authorities engaged in the investigation and prosecution of insurance fraud. In addition, CID designees are required to cooperate and respond promptly to requests made in the course of any criminal or civil investigation undertaken by the Minnesota Department of Commerce, law enforcement agencies, and/or authorized governmental agencies in accordance with all legal and regulatory requirements.

All referrals to the Minnesota Department of Commerce, law enforcement, and/or other authorized governmental agencies require CID management approval. Once the case is reviewed and approved, the paralegal or designee files the notification according to the agency requirements as set forth on its website and a copy of the referral is maintained in the case folder. In most cases, the referrals are submitted electronically through the National Association of Insurance Commissioners website. All referrals to law enforcement, regulators or state DOIs are included in the final case report and documented in CID's Investigative Case Management System ("ICMS").

VI. Civil Remedies

Prudential will pursue civil remedies for financial loss caused by fraudulent insurance acts, where appropriate.

Prudential has procedures to collect payments in cases prosecuted by law enforcement where restitution is ordered. CID, in cooperation with the business units and the Law Department,

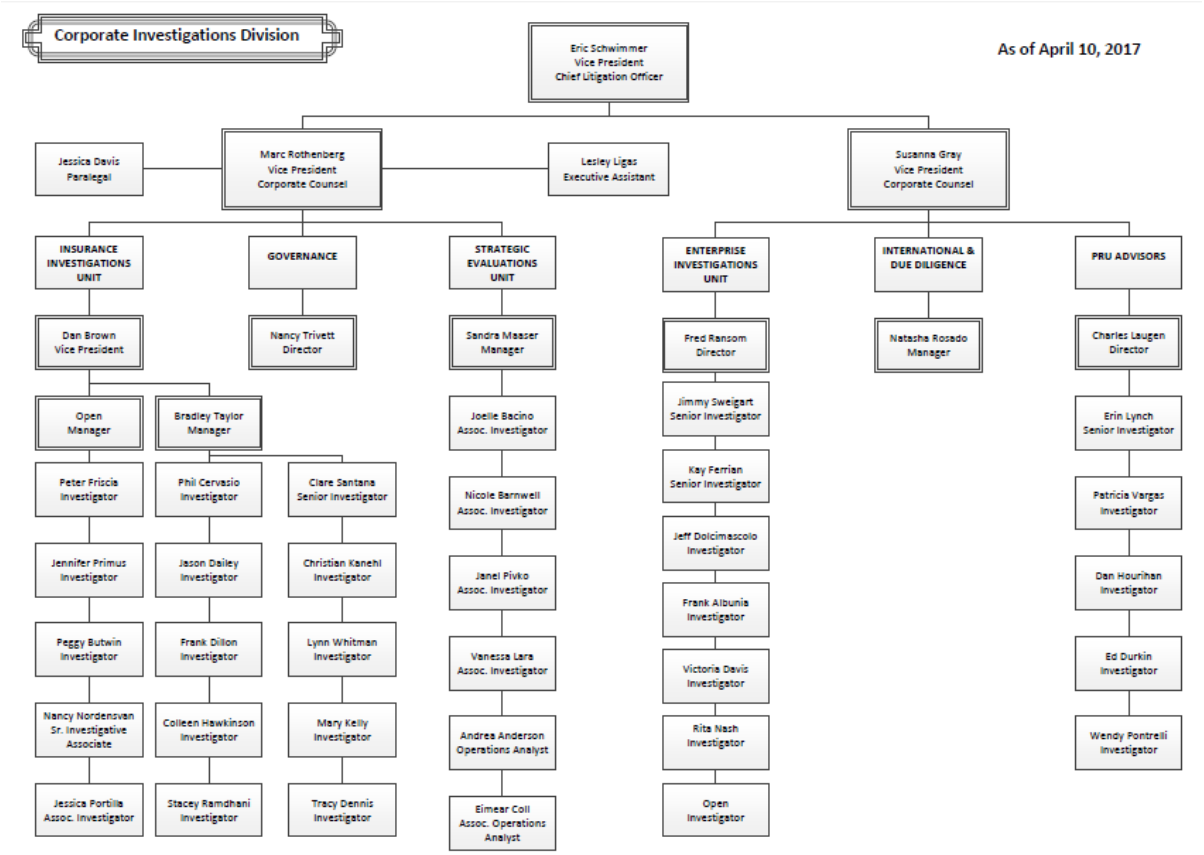
ensure that restituted funds are properly credited. Prudential monitors the receipt of all payments and works with the courts for their continued collection if delinquencies occur.

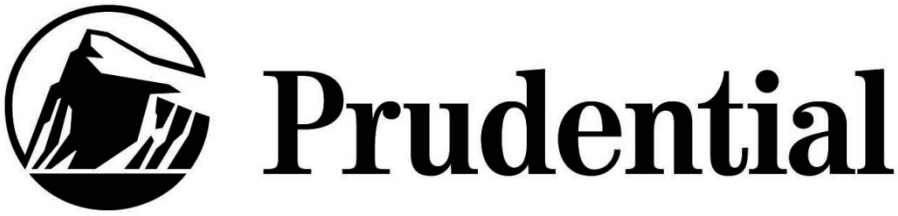
VII. Anti-Fraud Plan Review

CID reviews state Anti-Fraud Plans, including for the State of Minnesota, on an annual basis and files revised plans as required by law or regulation.

Exhibit A:

Corporate Investigations Division Organizational Structure




Prudential