

# Minnesota ANTI-FRAUD PLAN



# Prudential

## INTRODUCTION

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 .....	3
II.	Corporate Investigations Division/Individual Life Insurance SIU .....	5
III.	Referrals to the Minnesota Department of Commerce Fraud Bureau.....	13
IV.	Anti-Fraud Training Program .....	14

## I. Introduction

This plan has been revised in accordance with the requirements of Section 60A.954 of the Minnesota Statutes.

This plan contains information related to the Corporate Investigations Division (“CID”) and the Individual Life Insurance Special Investigations Unit (“ILI SIU”), which are both responsible for investigating and reporting fraud associated with the various Prudential entities identified on the cover page of this document to the Fraud Bureau of 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-, bank- 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 Policy and Controls

Prudential’s Fraud Prevention Policy (“Fraud Policy”), which is reviewed annually, 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.

Fraud is defined under the Policy “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.”

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.
- An internal auditing staff to search for and identify weaknesses in existing controls.

#### c. Employee and Customer Fraud Reporting

The Fraud Policy requires employees to “promptly report instances of known or suspected fraud, and cooperate with any internal or external investigations relating to 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 Corporate Investigations.”

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.

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](mailto:investigations@prudential.com)) can be found on the Company's website, through a dedicated "Report Fraud" hotlink.

d. Business Unit Fraud Prevention Policies

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 or the ILI SIU 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.

Additionally, the business units take intermediate steps prior to referring suspected instances of fraud to CID or the ILI SIU. For Individual Life Insurance Claims, suspected fraud is reviewed by senior management prior to submission to the ILI SIU. For Individual Life Insurance Underwriting, the Corporate Underwriters review prior to submission to the ILI SIU. For 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 the contract. In Group Insurance, upon suspicion of a claim fraud, a claim manager or underwriter should discuss 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.

**II. Corporate Investigations Division/Individual Life Insurance SIU**

Pursuant to Prudential's Fraud Policy, "CID has oversight responsibility for all fraud investigations conducted enterprise-wide and, within the U.S., for related regulatory reporting." Investigations with respect to the Annuities, Retirement and Group Insurance (Group Life, Disability and Long Term Care) divisions are handled by Prudential's CID. In addition, CID handles post-issuance Individual Life Insurance fraud investigations. In its role as the SIU for these businesses, CID has dedicated staff members whose primary responsibilities include investigating and reporting fraud connected to these products. CID is an independent function and sits within Prudential's Law, Compliance, Business Integrity and External Affairs Department ("LCBE").

Prudential's ILI SIU handles pre-issuance and claims investigations for the Company's Individual Life business. The ILI SIU sits within the Individual Life Insurance Business; however, it is independent from the Claims and Underwriting functions. Prudential's structure allows for sharing of information between CID and the ILI SIU so that a holistic approach to detecting and preventing insurance fraud is achieved. In early 2017, the ILI SIU will integrate into CID and will no longer exist within the Individual Life Insurance business.

Prudential will update its Anti-fraud Prevention and Detection Plan accordingly upon completion.

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, it is the shared mission statement of Prudential's Investigations functions:

“To detect, prevent and investigate activities that threaten Prudential and its customers.”

b. Responsibilities:

CID and the ILI SIU are responsible for:

- i. Conducting investigations related to suspected fraudulent activity by internal or external persons or entities;
- ii. Managing, directing and coordinating case referrals from within the different businesses;
- iii. Reporting investigative findings to relevant business stakeholders, including the risk, compliance, and legal functions;
- iv. When required, reporting to state Departments of Insurance, state Departments of Aging (or their equivalent), regulatory agencies, and law enforcement;
- v. Analyzing data from a centralized fraud reporting and case management database to provide risk assessment and trending of fraudulent activity;
- vi. Assessing risk and work with businesses and centralized business functions to mitigate risk; and
- vii. Developing and delivering training to integral anti-fraud personnel on issues relating to, among other things, the Company's fraud policy, “red flags” or characteristics of suspected fraudulent activity, and reporting of these activities for investigation by CID/ILI SIU.

c. Composition

*i. Corporate Investigations Division*

CID reports to the Chief Litigation Officer, Eric Schiwmmmer, and is co-led by Marc Rothenberg, VP & Corporate Counsel within CID. 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. CID investigations are also co-led by Susanna Gray, VP & Corporate Counsel. 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 29 associates:

- Vice Presidents (2)
- Directors (3)
- Managers (2)
- Senior Investigators (3)
- Investigators (10)
- Associate Investigators (4)
- Analysts (3)
- Paralegal (1)
- Executive Assistant (1)

CID's collective experience includes law enforcement, financial services, regulatory, compliance, and risk management. In addition, 7 members have advanced degrees (i.e. JD, MBA, MCJ, etc.) and 14 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](mailto:marc.rothenberg@prudential.com)

*ii. Individual Life Insurance Special Investigations Unit*

The ILI SIU reports to the Vice President of Underwriting, Investigation and Claims, Mike McFarland, and is led by Dan Brown, Vice President. Mr. Brown holds a Bachelors of Business Administration degree and has over 30 years of experience conducting investigations and managing investigators in the SIUs for various insurance companies, including over 10 years at Prudential.

The ILI SIU's staffing consists of 39 associates:

- Vice President (1)

- Director (1)
- Manager (1)
- Senior Investigators (3)
- Special Investigators (7)
- Associate Managers (4)
- Senior Investigations Associates (7)
- Senior Special Investigations Associates (2)
- Investigations Associates (13)

The ILI SIU's collective experience includes law enforcement, financial services, private investigations, and compliance. In addition, two members have advanced degrees (i.e. JD, MBA, etc.) and five are Certified Fraud Examiners. The ILI SIUs current organizational structure is attached as Exhibit B.

Within the ILI SIU, Dan Brown, Vice President, is the designated executive and primary contact person.

Dan Brown  
 Vice President  
 Individual Life SIU  
 13001 County Road 10  
 Minneapolis, MN 55442  
 (281) 558-5537  
 (281) 558-3934 (Fax)  
[dan.brown@prudential.com](mailto:dan.brown@prudential.com)

d. Qualifications

Members of CID and the ILI SIU performing investigations have the following requirements as minimum qualifications:

1. A Bachelor's degree in criminal justice or related field; or
2. An Associate's degree plus a minimum of two years of insurance claims investigation experience or professional investigation experience; or
3. A minimum of four years of professional investigation experience involving economic or insurance-related matters; or
4. A minimum of five years of law enforcement experience.

e. Associations and Memberships

Employees within CID and the ILI SIU 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)

f. Policies and Procedures

CID and the ILI SIU have established policies and procedures to ensure that allegations of fraudulent activity are thoroughly investigated and resolved, including reporting to state Departments of Insurance and outside regulatory and law enforcement agencies when appropriate (see Section III).

CID and the ILI SIU maintain Standard Operating Procedures (“SOPs”) in a corporate database available to all employees in each 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.

g. 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 which 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. Examples are:

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

The following is a non-exclusive list of indicators relating 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.

- 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 “[t]o 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 (6<sup>th</sup> 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 which 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;
- The negotiation of 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 relating to employee 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 somewhere other than the address of record;
- Partial or full surrender request indicates that the funds should be payable to an individual other than the owner(s), or directed to an account which 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/death 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 which 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/ILI SIU.

- The application contains misleading information which is relevant to the transaction request or claim;
- A beneficiary files a claim using suspicious documentation;

- An owner is found to possess multiple policies which 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 do 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 your calls at the residence during normal business hours;
- Individuals who have difficulty in keeping jobs;
- Information provided in the application or on the 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 relating 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 which 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.

#### h. Comprehensive Databases

CID and the ILI SIU subscribe to the following databases as part of their anti-fraud programs:

**LexisNexis Accurint:** Accurint provides comprehensive public and proprietary records information. It verifies essential personal identifiers, business records, professional licenses, nationwide bankruptcy, liens and judgments, property records, etc.

**Thomson Reuters CLEAR:** CLEAR is 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:** Searches are conducted 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.

**LexisNexis:** Applicant screening is provided for criminal record searches – county, state-wide, federal and international criminal record checks. Civil record searches are also conducted at the county and federal level. This service is in compliance with the Fair Credit Reporting Act (FCRA).

**MediConnect Global:** This is a record retrieval database service used to place and track orders for medical records obtained from various medical providers, such as doctors and hospitals.

**Pallorium/PallTech:** This is a comprehensive database that provides people finder services by name, date of birth, address, telephone and Social Security Number. Additional searches are available for businesses and corporations, criminal records, court searches, property records, etc.

**PACER Service Center:** Federal court records can be located for criminal, civil and bankruptcy cases.

**RegEd:** This database is used for broker due diligence.

**Search Systems:** This is a directory of links to public record databases and online services on the Internet.

### III. Referrals to the Minnesota Department of Commerce Fraud Bureau

Upon completion of an investigation, CID/ILI SIU will refer all suspected fraudulent insurance acts to the Minnesota Department of Commerce Fraud Bureau.

#### **IV. Anti-Fraud Training Program**

##### **a. CID and ILI SIU Investigator Training**

The members of CID and the ILI SIU receive Basic Entry Level training, which is no less than nine hours of classroom instruction. In addition, members of CID and the ILI SIU receive annual (continuing education) training of no less than nine 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 20 hours of training to maintain certification. External training involves attending or viewing specific training sessions in investigative techniques and practices, as well as participation in various industry associations, seminars, and conferences.

CID and ILI SIU investigators record their training received in an enterprise-wide training database called Learning Connection. Web Based Training (WBT) is facilitated by this system, which automatically logs completion of WBT courses. In addition to tracking each employee’s WBT courses, The Learning Connection database has a facility for investigations employees to record all of their external training and attendance at industry-related conferences.

CID and ILI SIU also sponsor internal training sessions for investigations members on proprietary systems, fraud trends, legal and compliance issues and significant investigations completed. Attendance at such training sessions is also logged and maintained.

##### **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 180 days of employment, Prudential provides a minimum of four and one-half (4.5) hours of instructor led new hire 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 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, red flags, events or circumstances present on a claim, (iii) 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. Non-Group Insurance

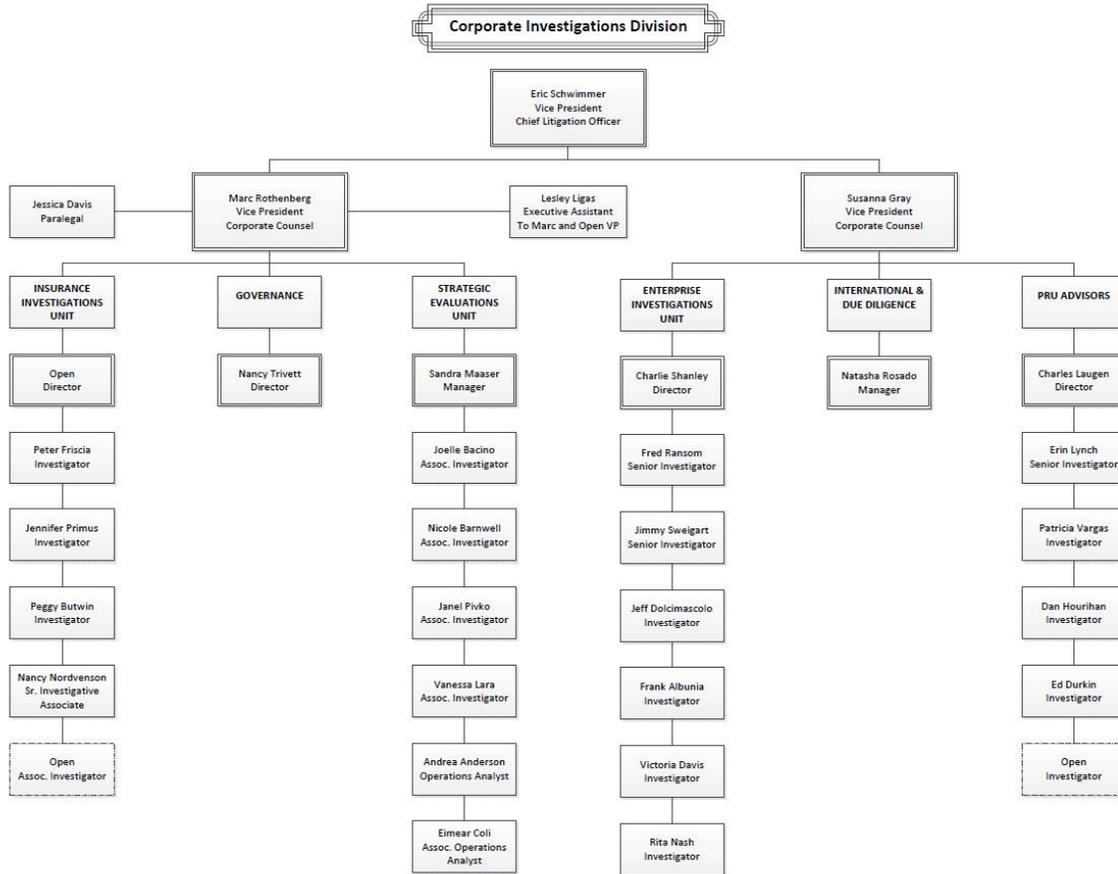
Prudential's integral anti-fraud associates, which includes among other functions, in businesses other than set forth in (b)(i) receive anti-fraud orientation within ninety (90) days of employment on the function and purpose of CID and the ILI SIU, overview of fraud detection and referral of suspected insurance fraud to CID and the ILI SIU, mandatory reporting requirements for various state departments of insurance, and organization charts for CID and the ILI SIU and contact telephone numbers. The Company has also developed five WBT courses available to all associates, with a course covering general fraud awareness and four additional courses tailored to specific job responsibilities such as Fraud Awareness for Individual Life Insurance, Group Insurance, Call Center, and Financial Professionals. Each WBT takes approximately a half hour to complete.

In addition, these associates receive a minimum of one hour annual fraud awareness training. The training session includes, among other things, education on CID/ILI SIU, the Company's Fraud Prevention Policy, "Red Flag" indicators of fraud, elder financial exploitation and money laundering, specific case examples, and steps to be taken by associates to refer suspected fraudulent activity to CID/ILI SIU.

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

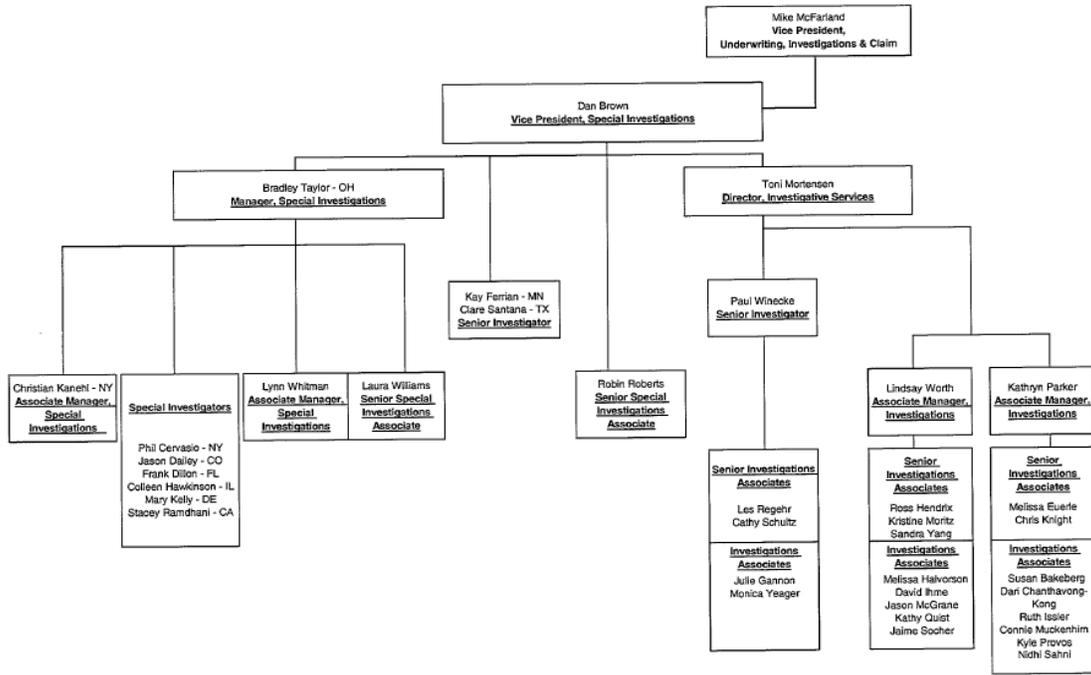
**Exhibit A:**

**Corporate Investigations Division Organizational Structure**



**Exhibit B:**

**Individual Life SIU Organizational Structure**





**Prudential**