Prudential

The Prudential Insurance Company of America
751 Broad Street
Newark, New Jersey 07102

January 3, 2025

VIA ELECTRONIC MAIL
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Dear Attorney General Brown:

Pruco Life Insurance of New Jersey ("Prudential") is writing to notify you of a recent data security incident that may have involved a limited amount of Personally Identifiable Information ("PII"), discussed in more detail below. Prudential is a financial services and insurance company headquartered in Newark, New Jersey. Please find below more detail and information about the incident and Prudential's response to the incident. Prudential is happy to discuss this incident with your office if necessary.

Description of the Incident:

We recently learned that between June and November 2024, an unauthorized individual was able to fraudulently access one of Prudential's websites by using information obtained through a non-Prudential source to impersonate financial professionals. This website was used by, but not required of, financial professionals of its third-party Broker-Dealers to manage relationships with individual customers who have purchased an annuity product. We took prompt steps to investigate the incident. The investigation determined that while accessing this website, the unauthorized individual was potentially able to view certain information that was accessible to these financial professionals. We conducted a review to determine what information was potentially able to be viewed by the unauthorized individual. On December 10, 2024, our investigation revealed that a limited amount of PII, including names, last four of Social Security numbers, email addresses, dates of birth, other information related to the annuity sold, and policy/contract/account number, was capable of being viewed by the unauthorized individual. We have not identified any evidence that the information has been misused.

Number of Individuals Involved:

Two (2) Maryland residents may have been impacted by this incident, were notified of the incident, and were mailed a notification letter via regular mail on January 3, 2025. A template copy of the notification letter is included with this letter as Exhibit A.

Steps Taken Regarding the Incident:

Prudential has taken steps to remediate the incident and mitigate the likelihood of this event occurring again in the future, including performing a manual lookback on all known fraudulent IP addresses associated with these events, deactivating any fraudulent financial professional accounts, increasing reporting metrics, implementing additional policy restrictions and fraud alerts for impacted customers, and deploying restrictions that will cause any fraudulent customer account attempts to fail. Prudential is also working to employ additional security controls in response to this incident. The impacted individuals were offered twenty-four (24) months of credit monitoring and identify theft restoration services through Kroll at no cost to the individual.

Other Information:

Prudential recognizes and appreciates the Attorney General's role in safeguarding Maryland residents, and Prudential takes the privacy and security of the PII in its control very seriously. Prudential hopes that the above information demonstrates its commitment to securing PII. Please let me know if you have any further questions and please do not hesitate to reach out directly to discuss any of this information.

Sincerely,

Logan Parker

Logan Parker
Vice President – Corporate Counsel
Prudential
Email: logan.parker@prudential.com
Phone: 1.816.694.7449

Enclosure

Exhibit A

Prudential

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Notice of Security Incident/Notice of Data Breach)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We, Prudential, write to inform you of a recent data security incident that may have involved a limited amount of information about you, including your name, address, and the policy and/or account number associated with the annuity product you purchased. We wanted to provide you with details about the incident, our response, and steps you can take.

What Happened?

We recently learned that between June and November 2024, an unauthorized individual was able to fraudulently access one of Prudential's websites by using information obtained through a non-Prudential source to impersonate your financial professional. We took prompt steps to investigate the incident. The investigation determined that while accessing this website, the unauthorized individual was potentially able to view certain information that was accessible to your financial professional. We conducted a review to determine what information was potentially able to be viewed by the unauthorized individual. On December 10, 2024, our investigation revealed that a limited amount of information about you, described below, was capable of being viewed by the unauthorized individual. We have not identified any evidence that the information about you has been misused.

What Information Was Involved?

Our review determined that the information capable of being viewed by the unauthorized individual was information associated with your annuity products, including your name, mailing address, date of birth, the last four digits of your Social Security number, the type of annuity product you purchased and related details, and the annuity policy and/or Prudential account number.

What We Are Doing?

We take the protection of information about you seriously. Upon discovering the incident, we revoked the unauthorized individual's access to the website. We also took prompt steps to help prevent this type of incident from occurring again in the future, including blocking individuals using fraudulent and suspicious IP addresses from logging into Prudential website accounts, and increasing fraud reporting and logging. Prudential is also working to employ additional security controls in response to this incident.

We have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

What You Can Do?

We encourage you to activate in free Kroll identity monitoring services. The enclosed Recommended Steps and Reference Guide provides information and activation instructions for the services available to you. Should you choose to activate, please use the Membership Number **<<Membership Number s_n>>**, valid for your use through <<b2b_text_6(activation deadline)>>.You will need to reference the Membership Number when activating, so please do not discard this letter.

We also encourage you to review the enclosed Recommended Steps and Reference Guide, which provides recommendations on how you can help protect information about you. The Recommended Steps and Reference Guide includes details on how to learn about identity theft, order and review your free credit report, report identity theft or fraud, place fraud alerts or security freezes on your credit file, and take advantage of state-specific resources.

For More Information?

If you have questions about this incident, you can contact us by calling 1-888-778-2888 between the hours of 8:00 am - 6:00 pm, ET (M-Fri).

On behalf of Prudential, we sincerely regret any concern or inconvenience this matter may cause you and appreciate your patience and understanding.

Sincerely,

Katie Feras
Vice President, Process Management
Annuities Service Center
P.O. Box 7960
Philadelphia, PA 19176

Recommended Steps and Reference Guide

Please review the information below and consider taking the steps noted.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

2. **Order And Review Your Free Credit Report.** You can remain vigilant by monitoring your free credit report, which you can order at www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by completing the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at https://consumer.ftc.gov/articles/free-credit-reports/ and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number, or request form. When you receive your credit report, review it carefully. Look for accounts you did not open, or inaccuracies in information about you. If you see anything inaccurate or that you do not understand, contact the consumer reporting agency.

3. **Report Identity Theft or Fraud.** You can remain vigilant by reviewing financial account statements for fraudulent transactions or identity theft. If you detect any unauthorized transactions in a financial account, promptly notify your financial institution. If you detect any incident of identity theft, promptly report the incident to law enforcement, the FTC, and your state Attorney General.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-438-4338, www.ftc.gov/idtheft/ and www.identitytheft.gov.

4. **Fraud Alerts on Your Credit File.** To help protect yourself from possible identity theft, consider placing a fraud alert on your credit file. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. For more information on fraud alerts, you can contact the consumer reporting agencies listed below or the FTC.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-685-1111* 1-800-525-6285† 1-888-298-0045‡	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742*‡ 1-800-311-4769†	www.experian.com
TransUnion	TransUnion Consumer Solutions P.O. Box 2000 Chester, PA 19016	1-800-909-8872* 1-800-680-7289† 1-800-916-8800‡	www.transunion.com

*General information

†Fraud alert information

‡Security freeze information

5. **Security Freezes on Your Credit File.** You have the right to place a "security freeze" on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. A security freeze must be placed on your credit file at each consumer reporting agency individually. For more information on security freezes, you can contact the consumer reporting agencies listed above or the FTC. As the instructions and fees (if any) for placing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. Placing a security freeze is free at the three nationwide consumer reporting agencies. Other credit reporting companies, for example employment or tenant screening companies, may charge a fee to place a security freeze based on your state laws. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide: your full legal name, Social Security Number, date of birth, addresses where you have lived in the past five years, copies of government-issued identification cards, and proof of your current address.

6. **State-Specific Information.**

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Maryland Residents. You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 528-8662, www.marylandattorneygeneral.gov.

For New York Residents. You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755 (toll-free), 1-800-788-9898 (TDD/TTY toll-free line), https://ag.ny.gov/, and at: Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, (212) 416-8433, https://ag.ny.gov/internet/resource-center/.

For North Carolina Residents. You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6000, www.ncdoj.gov.

For West Virginia Residents. You have the right to request a security freeze (charges may apply) as described above.