Prudential

March 29, 2024

BY U.S. MAIL

Office of the Attorney General
Consumer Protection Bureau
33 Capitol St.
Concord, NH 03301

To Whom It May Concern,

The Prudential Insurance Company of America ("Prudential") is providing this notice of a cybersecurity event to your office pursuant to N.H. Rev. Stat. § 359-C:20(I)(B).

On Sunday, February 4, 2024 an unauthorized third party believed to be associated with a cybercrime group obtained access to a Prudential employee's computer account by acquiring log-in credentials through social engineering of Prudential's help desk vendor. The unauthorized third-party subsequently acquired the log-in credentials of other Prudential employees. On Monday, February 5, 2024, Prudential became aware of this access, and promptly took steps to protect the integrity of its systems and data. Prudential activated its incident response plan and launched a forensic investigation, with the support of external cybersecurity experts, to assess the impact of and contain the incident. Prudential also reported the incident to the FBI, and is supporting the FBI in its investigation.

On February 14, 2024, Prudential identified evidence that the unauthorized third party removed certain customer information, potentially including personally identifiable information, from the network. On February 28, 2024, we determined that the affected data included individual

for residents of New Hampshire. At this time, we currently believe that approximately 91 New Hampshire residents were affected. Prudential's investigation and review of the affected data is ongoing, and Prudential anticipates additional rounds of notifications associated with this event. Prudential's monitoring has not revealed any indication that this personal has been leaked or otherwise misused for fraud or identity theft purposes.

Prudential began sending formal notification to the affected individuals via U.S. mail on March 29, 2024. Attached is a copy of the consumer notification mailed to the affected individuals in your state. Prudential is providing affected individuals with of complimentary credit monitoring and identity theft protection services through Kroll and establishing a dedicated call center to answer customer questions.

We have also taken, and will continue to take, proactive measures to protect our systems and data, including enhancing access controls and security protocols, and implementing additional monitoring technologies and procedures. Specifically, in order to mitigate the impact of incident, Prudential has reset all compromised accounts, reviewed and strengthened our conditional access policies, updated

password validation policies and procedures, and enhanced our password reset and MFA registration processes to include video verification, among other things.

If you have any questions, please contact me at .

Regards,

Marc Rothenberg
Vice President, Senior Regulatory Counsel

Prudential

[Date]

[*Recipient Name*]
[*Street Address*]
[*City, State, and Postal Code*]

Notice of [Security Incident/Data Breach]

Dear [First Name]:

At Prudential, we take seriously our commitment to protect the information we manage on behalf of our customers, employees, and company. We are writing to let you know we recently experienced a cybersecurity incident that affected some of your personal information.

We are providing you with information about the incident, our response, and additional measures you can take to help protect yourself. Importantly, we are not aware of fraud or misuse of your personal information resulting from this incident.

What Happened?

On February 5, 2024, Prudential detected unauthorized third-party access to certain company systems and data. We promptly activated our incident response plan and launched an investigation into the nature and scope of the issue with assistance from external cybersecurity experts. We also reported this matter to relevant law enforcement. Through the investigation, we learned that the unauthorized third party gained access to our network on February 4, 2024 and removed a small percentage of personal information from our systems.

What Information Was Involved?

Our investigation determined that information related to your Prudential products and services was affected by this incident. This information included your

What We Are Doing.

Prudential takes this incident and our responsibility to protect your personal information extremely seriously. As part of our response, we have worked with leading cybersecurity experts to confirm the unauthorized third party no longer has access to our company systems. We also have taken proactive measures to protect our systems and data, including enhancing access controls and security protocols, and implementing additional monitoring technologies and procedures, among other actions. We are also taking steps to strengthen our authentication protocols and help protect access to your account.

While we are not aware of identity theft or fraud related to information affected by this incident, as an additional precaution, we are providing you with of complimentary credit monitoring services. Details about this offer and instructions on how to activate these services are enclosed with this letter.

What You Can Do.

We encourage you to remain vigilant and review your account statements and free credit reports regularly to ensure there is no unauthorized or explained activity. We also encourage you to enroll in the complimentary credit monitoring services that we are offering. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains details about this offer and general guidance on what you can do to safeguard against possible future misuse of your information.

For More Information.

If you have additional questions, you may contact us at [contact information and hours of operation].

Sincerely,

Prudential

Steps You Can Take to Help Protect Personal Information

Enroll in Kroll's Monitoring Services

In response to this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 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, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services. *You have until* ***<<Date>>*** *to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

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

Additional Information

- **Credit Monitoring**. You will receive alerts when there are changes to your credit data—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 will be able to help you determine if it is an indicator of identity theft.
- **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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit- report-services/	https://www.experian.com/help	https://www.transunion.com/credit-
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For Massachusetts residents, under Massachusetts law, individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [#] Rhode Island residents that may be impacted by this event