Prudential

Kelly Harris
Vice President, Corporate Counsel

The Prudential Insurance Company of America
751 Broad Street
Newark, NJ 07102
(973) 802-6463

October 11, 2018

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To whom it may concern:

We are writing to inform you of a recent security matter involving six (6) New Hampshire residents/customers in accordance with N.H. Rev. Stat. §§ 359-C:19 – C:21; N.H. Rev. Stat. § 332-I:5 Standards for Safeguarding Customer Information.

Prudential provides an employer/Plan Sponsor (hereinafter referred to as "Client A") with 401k Plan recordkeeping services and maintains personal information of Client A's employees in connection with that relationship.

Due to a Prudential employee error, a data file containing personal information of Client A's employees was emailed to another Prudential client and that client's payroll vendor. Although the individuals at both the institutional client and payroll vendor who received this information ordinarily handles such information in their roles with their employers, they were not authorized to receive this information. Prudential has obtained written confirmation from both our client and the payroll vendor that the email and file containing this personal information was not saved or shared and has been deleted.

The information in the file attached to the email included the name, address, date of birth, Social Security number, employee ID, gender, marital status, and compensation of six (6) New Hampshire residents, all of whom will be receiving notice from Prudential of this incident and two (2) years of credit monitoring.

The Prudential employee who emailed this information in error has been counseled directly by management concerning this incident. In addition, management has ensured that the employee has completed both Prudential's mandatory compliance training as well as individualized training as a result of this incident.

Further, Prudential has commenced a review of current policies and procedures to reduce the risk of reoccurrence. Prudential will continue its fraud detection program, which includes account activity monitoring triggered by a combination of high risk activities (i.e., change of banking information) for our customers.

The nature of this incident does not require the filing of a police report, and there has not been any notification to other law enforcement agencies at this time.

If you have any questions, please feel free to call me at (973) 802-6463.

Very truly yours,

Kelly Harris

Prudential

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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Privacy Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to tell you about a data privacy incident that may have exposed some of your personal information. Prudential provides your employer with 401k Plan recordkeeping services and maintains your personal information in connection with that relationship. We take the protection and proper use of your information very seriously, which is why we are contacting you directly to explain the circumstances of the incident.

What happened?

Due to employee error a data file containing personal information related to your BT Americas 401(k) Plan was mistakenly emailed to another Prudential client and its payroll vendor. Although the individuals at both the institutional client and payroll vendor who received your information ordinarily handles such information in their roles with their employers, they were not authorized to receive your information. Prudential has obtained written confirmation that the email and file containing your personal information was not saved or shared and has been deleted.

What information was involved?

The information about you in the email included your name, address, date of birth, Social Security number, employee ID, gender, marital status and compensation.

What we are doing.

The Prudential employee who emailed your information in error has been counseled directly by management concerning this incident. In addition, management has ensured that the employee has completed both Prudential's mandatory compliance training as well as individualized training as a result of this incident.

Further, Prudential has commenced a review of current policies and procedures to reduce the risk of reoccurrence. Prudential will continue its fraud detection program, which includes account activity monitoring triggered by a combination of high risk activities (i.e., change of banking information) for our customers.

To help relieve concerns and restore confidence following this incident, we have also 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.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.
You have until January 7, 2019 to activate your identity monitoring services.
Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

What you can do.

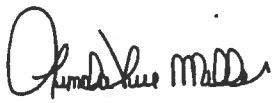
Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-877-778-2100, Monday through Friday from 8:00 a.m. to 9:00 p.m. Eastern Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,



LyndaSue Miller
Vice President, Data and Reporting | Full Service Solutions
Prudential Retirement

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll.

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 Internet Explorer, Chrome, Firefox, and Safari. 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.