[INCOM LETTERHEAD] 29634

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[ANY APPLICABLE CREDIT MONITORING PROMOTION CODE]

[DATE]

NOTICE OF DATA BREACH

Dear [INDIVIDUAL NAME]:

We are writing to notify you of a breach of security involving the unauthorized access of your personal information occurred on April 3, 2023, at our Vancouver, Washington facility.

WHAT HAPPENED?

Description

Incom's systems were breached by an unauthorized external individual who used a brute-force attack (a hacking method that uses trial and error to crack password and login credentials) to gain access to a legacy account credentials that had not been updated with DUO multifactor authentication. From there, the hackers used VPN to access files maintained on Incom's servers in Charlton, Massachusetts.

Incom's network monitoring software, DarkTrace, identified and interrupted the attack while it was in progress. After the cyberattack was successfully contained, Incom and DarkTrace's security experts conducted a full investigation to identify what information was impacted and to ensure that the threat was fully contained and neutralized. Unfortunately, during the course of our investigation we learned that a limited number of files were accessed and copied, including files that contained your personal information (described below), before DarkTrace was able to stop the cyberattack.

Remediation

After being alerted to this, Incom worked with its vendor, DarkTrace, to ensure we had all of the information and were interpreting it correctly. Specifically, Incom took the following actions:

- The VPN at the Vancouver facility was shut down after we were alerted to this on Tuesday April 4th and the appropriate changes were made to resolve the issue on April 6th.
- We verified the VPN at the Charlton, Massachusetts facility was configured correctly and secure.
- Network account credentials have been thoroughly examined and legacy accounts have been removed.
- All accounts have now been secured with DUO multifactor authentication.
- All users on the network have been forced to change their password to further ensure the internal network remains secure.

WHAT INFORMATION WAS INVOLVED?

DarkTrace was able to identify the specific information accessed and copied by the unauthorized user. You have received this communication because the data accessed by the unauthorized user included DarkTrace was able to identify the specific information accessed and copied by the unauthorized user.

You have received this communication because the data accessed by the unauthorized user included your first and last name along with your Social Security Number; and/or State Identification card number or Driver's license number; and bank account number that you provided to Human Resources for payroll.

WHAT WE ARE DOING

Incom values your privacy and deeply regrets that this incident occurred. Incom has implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of Incom's employees.

WHAT YOU CAN DO

Incom has arranged with ALLSTATE IDENTITY PROTECTION to provide you with credit monitoring/identity theft protection services for eighteen months, at no cost to you but you do need to enroll.

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on how to enroll for ALLSTATE IDENTITY PROTECTION as well as information about further steps you can take to protect your information including other credit monitoring/identity theft protection services.

FOR MORE INFORMATION

For further information and assistance, please contact Maura Grossman, Director, Human Resources at 508-909-2214 between 9 a.m.- 5p.m. [ET] daily.

Sincerely,

Michael A. Detarando, President & CEO

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241 Atlanta, GA 30374	P.O. Box 2002 Allen, TX 75013	2 Baldwin Place P.O. Box 1000 Chester, PA 19016

Credit Report Monitoring/Identity Theft Protection Services

In addition, INCOM has arranged with All State Identity Protection Program to provide you with credit monitoring/identity theft protection services for one year, at no cost to you.

ALLSTATE IDENTITY PROTECTION, **free of charge for 1 year**. Be sure to take full advantage of your complimentary identity and privacy protection plan by enrolling below.

Action Required: Enroll in Allstate Identity Protection coverage.

To help protect your identity and to maximize your protection, create your complimentary account by going to: www.MyAIP.com/ProtectIncom

Please note:

- This is for individual coverage for one year.
- If you are already enrolled in coverage, you will not need to re-enroll on the website. Your payroll deductions will stop during this one-year period of free coverage.

Once you enroll online, you will receive a Welcome email from customercare@aip.com with your Member ID and link to log in to your online portal. This is a legitimate communication, and you can expect to receive identity alerts from this email address in the future.

Your coverage includes:

- Comprehensive identity monitoring
- Credit monitoring
- Unlimited TransUnion reports and scores
- Dark web monitoring
- High-risk transaction monitoring
- Financial transaction monitoring
- Social media monitoring
- Allstate Security Pro℠ for real-time emerging threat alerts
- Allstate Digital Footprint℠ for privacy management
- Full service 24/7 fraud remediation
- Up to $1 million identity theft expense reimbursement
- Pre-existing conditions covered at no additional charge.

Questions?

If you have trouble logging in or have additional questions, please call Allstate Identity Protection at 800-789-2720 or email clientservices@aip.com. They are available 24 hours a day, 7 days a week to ensure that you have help when you need it most.

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://consumer.ftc.gov/identity-theft-and-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). [A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf].]

Police Report

Under Massachusetts law, you 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.

Security Freeze

In Massachusetts, you also have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a

result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;

8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.