

Payday America, Inc.
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

We value the relationship with our customers and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information.

WHAT HAPPENED?

On September 28th, 2021 we began experiencing outages and discovered that the company was the victim of a ransomware attack and some of our computer systems were compromised and encrypted. A forensic investigation determined that sometime on September 28th, 2021, a cybercriminal gained access to portions of the company's computer system and deployed various network reconnaissance and ransomware tools to gain access to portions of the system, and render them inaccessible to us. We have since restored our data from separate backup servers. The cybercriminal also informed us that they retained copies of much of the data and threatened to leak the information which could make it available to other cybercriminals.

WHAT INFORMATION WAS INVOLVED?

Subsequent analysis of the incident indicates that the data accessed by the unauthorized third party included, contact information, such as names, addresses, phone number and email address; driver's license numbers; and social security numbers.

WHAT WE ARE DOING

Payday America values your privacy and deeply regrets that this incident occurred. We have conducted a review of the potentially affected records and computer system, which review is ongoing, and we will notify you if there are any significant developments. We are working with cybersecurity experts to remove any remnants of this incident from our systems and improve our security. We have also informed law enforcement to ensure the incident is properly addressed.

We have opened a call center to answer any questions and provide additional information. The telephone number for the call center is 855-675-3112 and is available between the hours of 9am and 9pm Eastern Time, Monday through Friday.

WHAT YOU CAN DO

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information, 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 1-855-675-3112 between the hours of 9am and 9pm Eastern Time, Monday through Friday.

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

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
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

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 <http://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://www.consumer.ftc.gov/topics/privacy-identity-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.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Security Freeze

In some US states, you 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.