STINSON

Stephen Cosentino
PARTNER
DIRECT: 816.691.2450
OFFICE: 816.842.8600
steve.cosentino@stinson.com

November 19, 2021

Office of the Attorney General
ATTN: Data Breach Reporting
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040

Re: Notification of Data Security Incident

Dear Sir/Madam:

This firm represents Payday America, Inc. ("Payday America") located in Burnsville, Minnesota. We are writing to inform you about a data security incident involving our client, Payday America. Payday America is a company that provides payday loan services at various locations in Minnesota and online through its website at paydayamerica.com. After thorough investigation we have discovered customer information has been compromised. Accordingly, Payday America sent data breach notifications to residents in North Dakota who may have been affected by this incident. According to our records, a total of 12 North Dakota residents were impacted by this breach.

Description of the Incident

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 threat actor 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. On October 3, 2021, our third party ransomware incident response provider, Coveware, discovered that the threat actor exfiltrated personal information of the company. We have since restored our data from separate backup servers. The threat actor also informed us that they retained copies 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?

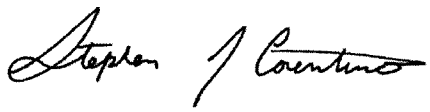
Upon notification of this breach, we immediately launched our own investigation and have taken the following steps:

- We have conducted a review of the potentially affected records and computer system, which review is ongoing, and we will notify our customers 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 informed law enforcement to ensure the incident is properly addressed;
- We have provided free identity monitoring services through our service provider, Epiq, for those individuals that qualify for such services under state requirements; and
- 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.
- We have updated our written information security policy.
- We have deployed Cortex cyberincident detection software from our third party forensic investigation provider, Palo Alto Networks – Unit 42.

For your reference, we are including a copy of the notice letter to consumers that was mailed to the affected individuals between November 19 and November 22, 2021. Please contact me if you have further questions.

Sincerely,

Stinson LLP



Stephen Cosentino
1201 Walnut Street
Suite 2900
Kansas City, MO 64106

Enc.

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.

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). You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

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.

You may also contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/.

State specific resources:

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.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your 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 Rhode Island residents: You may contact the Rhode Island Office of the Attorney General at 401-275-4400, https://riag.ri.gov/.

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.

For Rhode Island Residents: You have the right to file and obtain a police report if you are a victim of identity theft.

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 http://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

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).

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	P.O. Box 2002	2 Baldwin Place
Atlanta, GA 30374	Allen, TX 75013	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.