[AUTOPAY Logo]
[AUTOPAY Address]

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Notice of Data Breach

Dear [Insert customer name]:

I am writing to you on behalf of AUTOPAY Direct, Inc. ("AUTOPAY") with important information about a data security incident that occurred recently. AUTOPAY takes the protection and proper use of your personal information very seriously. We are, therefore, contacting you to explain the incident and provide you information about security measures you can take to protect yourself and your personal information.

What Happened:
On February 5, 2022, a threat actor group notified us that it had infiltrated our internal network and extracted certain data, including personally identifiable information of some of our customers. The group threatened to release the data online unless their ransom demand was met; however, in accordance with the standard recommendation of the FBI and financial regulators, we did not pay the ransom. We promptly retained an outside forensic firm to conduct a thorough investigation, determine the systems impacted, and contain and remediate the incident, including terminating all unauthorized access to our systems. The forensic firm determined that the data was exfiltrated over a two-day period, starting on February 2, 2022 and ending on February 3, 2022. Over the next several weeks, we undertook a comprehensive data analysis effort to identify any sensitive data that may have been impacted. This notice was not delayed as the result of a law enforcement investigation.

What Information Was Involved:
This incident involved certain of your personal information, including [<<LIVE FIELD>> PICK FROM THE FOLLOWING, AS APPROPRIATE: your name, street address, Social Security number, driver's license number and date of birth]. As a result, your personal information may have been exposed to others.

What We Are Doing:
We have taken, and are continuing to take, actions to mitigate this incident and to protect against similar attacks in the future. Such actions include: notifying law enforcement, successfully terminating all unauthorized access, undertaking a full forensic investigation of the incident, implementing multifactor authentication for all users across the organization, and configuring additional security measures on our information technology platforms (including enhanced password management, access control restrictions and updated logging capabilities).

For More information:
Please review the "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 (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also report any suspected incident of identity theft to law enforcement and you can obtain a copy of any resulting police report. If you do suspect that you have been the victim of identity theft, you should also notify your state Attorney General and the FTC.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at **[customer service number]**.

Sincerely,
Jeff Hutcheson
Chief Executive Officer

Additional Resources

Information on Obtaining Credit Reports, Credit Freezes and Security Alerts

It is important that you remain vigilant over the next 12 to 24 months by reviewing your account statements and monitoring your free credit reports for suspicious activity. We have provided information below about how to contact the credit reporting agencies and the Federal Trade Commission to obtain your credit report, place fraud alerts and credit freezes, and obtain additional information.

Obtain a Free Credit Report: You may obtain a free copy of your credit report from each of the three nationwide consumer reporting agencies by calling 1-877-322-8228 or going online to www.annualcreditreport.com. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies.

Credit Freezes & Fraud Alerts: You have a right to place a 'security freeze' on your credit report at no charge, which will prohibit a credit reporting agency from releasing information in your credit report without your written authorization. The security freeze is designed to prevent credit loans, and services from being approved in your name without your consent. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prohibit the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other accounts involving the extension of credit. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. To place a security freeze on your credit report, you must contact **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) 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:

Experian: (888) 397-3742 Experian Security Freeze P.O. Box 9554 Allen, TX 75013 https://www.experian.com/freeze/center.html	**Equifax: (877) 298-0045** Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 https://www.equifax.com/personal/credit-report-services/credit-freeze/	**TransUnion: (888) 909-8872** TransUnion Credit Freeze P.O. Box 160 Woodland, PA 19094 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 agencies, 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 years, the addresses where you have lived over the prior five years, (5) 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 three (3) business days after receiving your request to place a security freeze on your credit report. 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.

To learn more about fraud alerts, security freezes, and protecting yourself from identity theft and to report incidents of identity theft, you can visit the Federal Trade Commission's website at www.consumer.gov/idtheft, or www.ftc.gov/credit, or call 1-877-IDTHEFT (1-877-438-4338). You may also receive information from the Federal Trade Commission by writing to: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You also have a variety of rights under the federal Fair Credit Reporting Act (FCRA). For more information on your FCRA rights, visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

For residents of the following states, your state's statute requires that we notify you that you may also obtain information about preventing and avoiding identity theft from your State Attorney General's Office or other state resource listed below:

- Maryland: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us
- North Carolina: North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov
- New York: New York Division of Consumer Protection, consumer hotline 800-697-1220, https://www.dos.ny.gov/consumerprotection/security_breach/data_security_breach.htm
- Rhode Island: RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400; http://www.riag.ri.gov/ConsumerProtection/About.php#
- Washington DC: Office of the Attorney General for the District of Columbia: https://oag.dc.gov/ .