City of Medford
City Attorney's Office

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>>

Notice of Data Breach

Dear <<Name 1>>,

This notice is to make you aware that the City of Medford has been impacted by a data incident, which may have resulted in an unauthorized individual gaining access and installing software that was designed to capture payment information as it was inputted on our website. We wish to provide you information on steps you can take to protect yourself and minimize the possibility of misuse of your information.

According to a forensic investigation, the incident could affect individuals who made credit or debit card payments to the City of Medford between February 18, 2018, and March 14, 2018 and between March 29, 2018 and April 16, 2018. Please note that because we do not collect sensitive personal information like Social Security numbers, this type of sensitive information was not affected by this incident.

We regret that this incident occurred and we are working diligently to resolve this incident. Upon learning of this incident, we immediately commenced a forensic investigation and took steps to address and contain this incident.

What Happened

Based upon an independent forensic investigation, it appears that an unauthorized individual was able to gain access to portions of our website and install software that was designed to capture payment card information as it was inputted on the website. We believe the incident affected only credit and debit card payments to the City made between February 18, 2018, and March 14, 2018 and between March 29, 2018 and April 16, 2018.

What Information Was Involved

We believe that malware was used to gather payment card information, which may include credit or debit card numbers, cardholder names, card expiration dates and CVV codes, from our website's payment-related systems between February 18, 2018, and March 14, 2018 and between March 29, 2018 and April 16, 2018.

The City of Medford does not collect social security numbers or federal or state identification numbers from these systems. Therefore, this personal information was not affected by this incident.

What Are We Doing

Upon learning of this incident, we immediately commenced a forensic investigation and took steps to address and contain this incident. We temporarily disabled website payments while our investigation was underway. We restored payment services after addressing this incident.

What You Can Do

We recommend that you review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities. In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Although Social security numbers and similar sensitive personal information were not at risk in this incident, as a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As an additional precaution, we are providing information and resources to help individuals protect their identities. This includes an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

For more information about this incident, or if you have additional questions or concerns, please feel free to contact our dedicated call center at 844-808-4890 between the hours of 6 a.m. and 6 p.m. Pacific Time, Monday through Friday.

Once again, we sincerely regret that this incident occurred.

Sincerely,

Eric B. Mitton
Deputy City Attorney

Information about Identity Theft Protection

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

> **For residents of North Carolina**: You may also obtain information about preventing and avoiding identity theft from 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.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)

General Contact:
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)

General Contact:
P.O. Box 105281
Atlanta, GA 30348
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872