

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>>:

El Paso-Los Angeles Limousine Express, Inc. understands the importance of protecting and securing the payment card information of our customers. We are writing to inform you of a recent incident that may have involved that information and to explain steps that you can take to help protect your information.

#### **What Happened and What Information Was Involved**

On September 10, 2018, Wells Fargo informed us that our website handling our company's online ticket sales (<https://ims.eplalimo.com>) was a common point of purchase for some unauthorized credit card transactions with other merchants and that there may have been a possible compromise of our website. We immediately began an investigation with the assistance of a leading computer security firm. On September 13, 2018, the vendor that we hired to manage and host our online reservations determined that a coding error by a developer had created the potential for unauthorized access to payment card data stored on our website. Specifically, information you provided during checkout including name, address, email address, payment card number, expiration date, and printed card security code, was accessible to unauthorized parties. Based on our investigation, we believe the incident only involved customers who bought or attempted to buy tickets on our website between December 9, 2016 and September 13, 2018. We are notifying you because you bought or attempted to buy a ticket during that time period using a payment card.

On September 18, 2018, our investigator learned that our website had been the common point of purchase for a larger number of unauthorized credit card transactions for a different credit card brand. We were not aware of any customer complaints regarding credit card use on our website prior to hearing from Wells Fargo on September 10, 2018. While we have not been able to actually verify that our website was the cause of any of these unauthorized transactions, we are notifying you out of an abundance of caution so that you can take steps to protect and secure your credit card information.

#### **What We Are Doing About It**

We take the security of our customers' personal information very seriously. First, we immediately began working with our forensic investigator and vendor to find out what had happened. By September 13, 2018, our vendor had identified and corrected the error that caused this issue and made sure that the data was no longer accessible to unauthorized parties. To help prevent a similar incident from occurring in the future we will continue to conduct a review of our website and will further enhance the security measures for our website as needed. In addition, we are working with the payment card networks so that banks that issue payment cards can be made aware.

## **What Can You Do**

If you believe your credit card information may have been compromised, you should consider contacting your credit card company and/or financial institution and request that the card be reissued with a new printed card security code, replaced with a new credit card number, or be cancelled. You may also contact law enforcement. We recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing and monitoring your account statements and free credit reports for any unauthorized activity. We ask that you review the attached sheets called More Information About Identity Theft and Ways to Protect Yourself and State Specific Information for more information.

## **For More Information**

If you have any questions or need more information, please call our hotline number 888-238-5408 Monday through Friday, from 6:00 a.m. to 6:00 p.m. PST.

We sincerely apologize for any inconvenience and concern this incident has caused you. Our team is working to help prevent similar occurrences in the future. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Very Truly Yours,



Jerry Rosenbaum, President

/enclosures

## MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding identity protection. You can obtain additional information about preventing identity theft from the Federal Trade Commission by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. The FTC also provides information online at <https://www.consumer.ftc.gov/features/feature-0014-identity-theft> or you may contact them at: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

### National Credit Reporting Agencies Contact Information

<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30374-0241 1-800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 2002 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 6790 Fullerton, CA 92834-6790 1-800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>
---	---	--

You can get information about fraud alerts and security freezes from the FTC and the Credit Reporting Agencies.

### **Obtain Your Credit Report**

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national credit reporting agencies. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the credit reporting agency delete that information from your credit report file.

In addition, 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. You may obtain a free copy of your credit report by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at [www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf](http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf), and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

### **Place a Fraud Alert or Security Freeze on your Credit Report File**

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to apply for credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the national credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding placing a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. For state-specific security freeze information, you can visit <http://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/>.

### State Specific Information

**IOWA residents:** You may contact law enforcement of the Iowa Attorney General's Office to report suspected incidents of identity theft. This Office can be reached at:

Office of the Attorney General of Iowa  
Hoover State Office Building  
1305 E. Walnut Street  
Des Moines, IA 50319  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)  
(515) 281-5164

**MARYLAND residents:** You may obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This Office can be reached at:

Office of the Attorney General  
Consumer Protection Division  
200 St Paul Place  
Baltimore, MD 21202  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)  
(888) 743-0023

**NEW MEXICO residents:** You have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit: [www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf) or [www.ftc.gov](http://www.ftc.gov).

In addition, you also have the right to obtain a security freeze or submit a declaration of removal under the New Mexico Fair Credit Reporting and Identity Security Act. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft.

**NORTH CAROLINA residents:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice  
Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
[www.ncdoj.gov](http://www.ncdoj.gov)  
(877) 566-7226

**OREGON residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice  
1162 Court Street NE  
Salem, OR 97301-4096  
[www.doj.state.or.us](http://www.doj.state.or.us)  
(503) 378-4400

**RHODE ISLAND residents:** You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at:

RI Office of the Attorney General  
150 South Main Street  
Providence, RI 02903  
[www.riag.ri.gov](http://www.riag.ri.gov)  
(401) 274-4400

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.