[Insert Date]

««First Name Last Name»»
««Address»»
««City, State, Zip»»

Dear ««First Name Last Name»»,

We are writing to provide a follow up on a previous notification from Global Payments, Inc. ("Global Payments") regarding a security incident concerning the unauthorized access of payment card information.

Specifically, Global Payments informed Comerica in June that their ongoing investigation revealed potential unauthorized access to its servers that contain merchant application data. Global Payments recently provided Comerica with the details regarding the individuals potentially affected. As part of our Merchant Card services, you provided personal information on your merchant application submitted both to Comerica Bank and Global Payments. The merchant application was provided by you so Global Payments could engage in credit underwriting for Comerica Bank and Global Payments. The personal information on your merchant application may have included your name, social security number and the business bank account number(s) designated for the deposit of merchant processing proceeds.

As stated in the notification you received from Global Payments, it is unclear whether the intruders looked at or took any personal information from their systems. However, because your social security number may have been compromised, we encourage you to take advantage of the credit monitoring and identity protection insurance Global Payments is offering, at no cost to you for one year, through Equifax Personal Solutions. If you have not already signed-up for this free product, you may sign-up by using the promotion code from the Global notice or the following promotion code **413647645** by visiting www.myservices.equifax.com/3in1alerts and following the steps described. If you require additional information regarding this incident, please call **800-697-1159** between 9:00 a.m. and 9:00 p.m. Eastern time, Monday through Friday.

We suggest that you be vigilant over the next 12 to 24 months and promptly report any incidents of suspected fraudulent activity or identity theft. In addition, we encourage you to monitor the business bank account(s) that were designated for the deposit of merchant processing because those account(s) may have also been compromised. You may want to contact your financial institution and tell them that your account(s) may have been compromised and ask that they flag or close your account(s). If your account resides at Comerica Bank and you wish to discuss closing that account and opening a new one, please contact your Relationship Manager at Comerica. We will, of course, accommodate your request at no charge to you.

We have provided additional information regarding identity theft prevention, detection and defense on the reverse side of this notice.

We apologize for any inconvenience you may experience as a result of this incident. For more information regarding this security incident, visit www.2012infosecurityupdate.com. If you have questions concerning your banking relationships, please contact your Comerica Relationship Banker directly or Comerica Merchant Services at 888-591-5099 between the hours of 9:00 a.m. and 5:00 p.m. PT.

Sincerely,

Susan C. Schmidt
Senior Vice President
Corporate Quality Process Department

Supplemental Identity Theft Prevention Information

Free Credit Reports:
You can order credit reports once a year at no charge from the national credit reporting companies by visiting www.annualcreditreport.com, by calling 877.322.8228, or by completing the Annual Credit Report Request Form (which can be printed from www.ftc.gov/credit) and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Upon receiving your credit report, review it carefully. If you see anything you do not understand, call the credit reporting agency at the telephone number listed on the report. Errors may be a warning sign of possible identity theft. If there are accounts or charges you did not authorize, immediately notify the appropriate credit reporting agency by telephone and in writing.

Fraud Alerts:
A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You may place fraud alerts on your credit files by contacting any one of the three national credit reporting agencies listed below:

Equifax P.O. Box 740241 Atlanta, GA 30374-0241	www.equifax.com	800.525.6285
Experian P.O. Box 9532 Allen, TX 75013	www.experian.com	888.397.3742
TransUnion Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790	www.transunion.com	800.680.7289

Credit Freeze:
You have the right to put a credit freeze (security freeze) on your credit file by contacting the three national credit reporting agencies listed above so that no new credit can be opened in your name without the use of a PIN number issued by a consumer reporting agency. A credit freeze is designed to prevent potential creditors 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, placing a credit freeze on your credit report may delay your ability to obtain credit. You may incur fees to place, lift, and/or remove a credit freeze. The cost of placing, temporarily lifting, and removing a credit freeze varies by state and generally ranges from $5 to $20 per action at each credit reporting agency.

Contacting the Federal Trade Commission (FTC):
To learn more about how to protect yourself from becoming a victim of identity theft, contact the FTC by using the information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1.877.IDTHEFT
http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/index.html

Law Enforcement:
If you believe you are a victim of identity theft, promptly report the matter to your local law enforcement.