<<FULLNAME>>
<<COMPANY>>
<<AA1>>
<<ADRRESS>>
<<CITY,STATE,ZIP>>
<<IMB BARCODE>>

Dear [Insert Name]:

We are writing to inform you of a security incident involving certain personal information you provided while shopping at Wireless Emporium.com (the "Website"). As a precaution we are providing this notice and outlining some steps you may take to help protect yourself. We sincerely apologize for any inconvenience or concern this may cause you.

On July 1, 2014, we learned that unauthorized individuals or entities installed malicious software on our Website computer server and took payment card data. We believe the malware could have compromised the payment card data of visitors that made purchases through the Website between December 24, 2013 and January 19, 2014, including name, address, payment card account number, card expiration date and security code. According to our records, you made a payment card purchase at the Website during that timeframe, and your information may be at risk.

Keeping your personal information secure is of the utmost importance to us, and we took steps to address and contain the incident as soon as it was discovered. We also engaged a computer forensic investigator to perform an investigation, and we have already taken measures designed to prevent this from happening again the future, such as installing a new firewall and updating the code we use to run the Website.

We want to make you aware of steps you can take to guard against identity theft or fraud. We recommend that you review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

We recommend that you carefully check your credit reports for accounts you did not open, for inquiries from creditors you did not initiate, and personal information, such as home address, that is not accurate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. Also, please review the enclosed "Information about Identity Theft Protection" reference guide that describes additional steps you may take to help protect yourself, 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.

Finally, if you have any questions or concerns you may call the privacy hotline at (800) 760-1464 between the hours of 9:00 AM and 5:00 PM (Pacific Time), Monday through Friday (excluding holidays), to address additional questions or concerns you may have. Again, we are sorry for any inconvenience or concern this event may cause you.

Sincerely,

The Wireless Emporium Team
www.wirelessemporium.com
PO Box 6087
Orange, CA 92863
(800) 760-1464
privacy@wirelessemporium.com

Information about Identity Theft Protection

We recommend that you 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 below.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790
800-685-1111 ; www.equifax.com	888-397-3742; www.experian.com	800-916-8800; www.transunion.com

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 us and 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 Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 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

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 below:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 6790
877-478-7625; www.equifax.com	888-397-3742; www.experian.com	Fullerton, CA 92834-6790
		800-680-7289; www.transunion.com

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.

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	Fraud Victim Assistance Division
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 6790
www.equifax.com;	www.experian.com	Fullerton, CA 92834-6790
		www.transunion.com

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