



[Cardholder Name]
[Address]

Notice of Data Breach re [STORE NAME] - Important Security and Protection Notification from MedAltus. Please read this entire letter.

Dear [cardholder name]:

At MedAltus LLC, we value the trusted relationship we have with every client, every distributor and every vendor. It is a core value at MedAltus that we act with honesty and integrity in all that we do. That's why I wanted to take a moment to let you know about a recent data security incident.

What Happened / What Information Was Involved

Our records indicate that you have recently purchased products through the online store called [STORE NAME] located at [website address]. Essentially, our Ecommerce platform related to this store has been illegally hacked into by outside intruders. Beginning at least as early as May 3, 2016, we believe MedAltus order information may have been improperly intercepted/accessed from our Ecommerce website. This order information may have included your name, address, email, phone number, fax number, credit card information and any username or password that you may have created to access the site and purchase products. As a result, this information may have been potentially exposed to others.

Because the breach occurred very recently, the investigations are still ongoing. However, we do know that one or more parties illegally accessed our Ecommerce site and inserted a script to allow such parties to intercept information being transferred to our payment processor, including purchaser's names, credit card numbers and other related information. We have no information to indicate that any card has yet incurred any unauthorized charges.

What We Are Doing

Please be assured that we are taking appropriate steps necessary to address the incident, and that we are committed to protecting the information that you have entrusted to us. We have retained the services of an experienced cyber security and forensic investigative firm to fully investigate the incident. Following recommended protocols, we have reported the matter to federal law enforcement authorities, including the Electronic Crimes Task Force of the United States Secret Service.

To better protect you and your information, we have taken immediate steps to further secure all data. Since discovering the breach, MedAltus has taken immediate action to remove any system vulnerabilities, including deleting the compromised administrative user, changing relevant administrative passwords, installing security patches, and increasing tracking and monitoring of activity.

We regret any inconvenience this incident may have caused you. We are committed to working with authorities to do all we can to help protect our customers.

For More Information

Should you have questions or concerns regarding this matter or the protections available to you, please do not hesitate to contact us at 1-800-393-3848 (8am-5pm EST). Also attached to this letter is further information that you may find helpful.

Sincerely,



Lee Jacobson, COO
MedAltus, LLC

[Attachment]

ADDITIONAL INFORMATION
YOU HAVE RECEIVED A DATA BREACH NOTICE – WHAT YOU CAN DO

Now that you have been notified that your personal information may have been exposed in a data breach, you should be aware that there are steps you can take to help protect yourself from identity theft.

- First, you should immediately contact your bank or credit card company to cancel the card that you provided to us and request a new one. If you are unsure which card you used on our website, please contact us at 1-800-393-3848.
- You should vigilantly review your account statements and transactions regularly and make sure that no one misused your card. If you find fraudulent charges, call the fraud department and get them removed.
- If you have automatic payments set up, update them with your new card number.
- Request and check your credit report at annualcreditreport.com or call 1-877-322-8228. If you have not ordered a report in the past year, it is free. If you have already ordered your free annual reports this year, you can pay to get your report immediately from one of the credit bureaus listed below, or you may be entitled to another free report if you have placed a fraud alert on your credit report recently. You may also want to check with your credit card company, as they may provide free services. Credit reporting services can vary in fees.
- Contact one of the three credit bureaus and place a fraud alert. A fraud alert is free. It will make it harder for someone to open new accounts in your name. You should get a letter from each credit bureau that will confirm that they placed a fraud alert on your file. If you contact one of the companies below, they must tell the other two.
 - Equifax
www.equifax.com/CreditReportAssistance/
P.O. Box 740250
Atlanta, GA 30374
1-888-766-0008
 - Experian
www.experian.com/fraud/center.html
P.O. Box 1017
Allen, TX 75013
1-888-397-3742

- Trans Union
www.transunion.com/fraud
PO Box 2000
Chester, PA 19022-2000
1-800-680-7289

If you suspect that identity theft has already occurred and that your card has been, or is being, used improperly, you should consider taking the following steps:

- Call the companies where you know fraud has occurred and alert the fraud department. Ask them to immediately close or freeze the account if you haven't already.
- Contact the Federal Trade Commission (FTC), your state's Attorney General or other forms of law enforcement. The FTC has an online complaint form located at its website shown below. The FTC also provides useful information for filing a police report on its website.

We strongly encourage you to visit the Federal Trade Commission's Identify Theft Information website located at <https://www.identitytheft.gov/>, as well as the websites for the reporting agencies listed above, for further information on topics such as placing fraud alerts and security freezes. You can also contact the FTC at 1-877-ID-Theft (438-4338) or at:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580