

June 13, 2016

STATE OF NH  
DEPT OF JUSTICE  
2016 JUN 16 AM 11:35

Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Dear Attorney General:

**NOTICE OF A DATA BREACH**

Between 5/4/2016 and 5/19/2016 hackers placed malware code on our tiemart.com website. On 6/3 we were able to determine that the code was electronically sending names, addresses and credit card information to an unknown third party location.

**NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED**

This breach affected a total of 927 individuals of which 7 were residents of New Hampshire. These residents will shortly receive notice via US mail. All notices are being mailed out today.

**STEPS WE HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT**

Since this breach we have taken the following steps:

1. Malicious code deleted.
2. All admin user passwords reset and expire every 90 days.
3. Implemented additional server level password to access admin of application server.
4. Reset passwords on all affected user accounts.
5. Began daily scans of site using Comodo Hackerproof.
6. Investigating additional ways to alert us if the website is modified to ensure that similar incidents do not occur in the future.

We have no evidence that any of the personal information has been used for fraudulent purposes.

A police report has been filed with the Mundelein, IL police department. The report # is 16-05204. Taken by officer Trevor McElroy, 221 North Lake Street, Mundelein, IL 60060. 847-968-4600.

We will be offering Transunion Credit Monitoring services at no charge to the affected New Hampshire residents.

**OTHER NOTIFICATION AND CONTACT INFORMATION**

If there are any questions or you need further information, please contact myself, Mike Martyka. My email is [mike@tiemart.com](mailto:mike@tiemart.com). My phone is 847-566-5980 extension 305.

Sincerely,



Michael G. Martyka

President, Tiemart, Inc.

June 13, 2016

<FIRST NAME> <LAST NAME>  
<ADDRESS1>  
<ADDRESS 2>  
<CITY>, <STATE> <ZIPCODE>

Dear <FIRSTNAME> <LASTNAME>:

**Please read this letter in its entirety.**

We were recently made aware of a situation that may have exposed certain payment card information on our website. We are notifying you of the fact that the payment card you used with us was one of the affected cards impacted by this situation. This payment card information includes customer name, address, credit card number, credit card expiration date and security code.

**While we have no evidence that any of your personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.**

**What is TieMart, Inc. doing to address this situation?**

TieMart, Inc. has made immediate enhancements to our systems, security and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that appropriate security protocols are in place going forward. TieMart, Inc. is committed to helping our customers. That's why TieMart, Inc. is providing you with access to **Single Bureau Credit Monitoring\*** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. These services will be provided by **IDT911**, a company that specializes in identity theft education and resolution.

**How do I enroll for the free services?**

To enroll in **Credit Monitoring\*** services at no charge, please log on to [https://www.myidmanager.com/promo\\_code.html](https://www.myidmanager.com/promo_code.html) and follow the instructions provided. **When prompted please provide the following unique code to receive services: <CODE HERE>**

To take advantage of the **IDT911** services, or to obtain additional information about these services, **please call the IDT911 help line 1-800-405-6108** and supply the fraud specialist with your unique code.

**What can I do on my own to address this situation?**

**We are strongly urging all customers** to notify their issuing bank of this incident to inform them that your account may be at an increased risk for fraud and so they can flag your account. We also encourage you to monitor your account closely for any suspicious activity and to notify your financial institution immediately if you notice any unauthorized spending or withdrawals.

\* Services marked with an "\*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection and in order to confirm your identity.

State law allows consumers to place a fraud alert on their credit reports. A fraud alert is a cautionary flag, which is placed on your credit file to notify lenders and others that they should take special precautions to ensure your identity before extending credit. When you place a Fraud Alert, you can provide a mobile or other phone number for lenders to contact you to verify that the party applying for credit is actually you, not a fraudster.

**If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:**

- Experian (1-888-397-3742)
- Equifax (1-800-525-6285)
- Transunion (1-800-680-7289)

**Also, should you wish to obtain a credit report and monitor it on your own:**

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to TieMart, Inc.

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

**What if I want to speak with TieMart, Inc. regarding this incident?**

While IDT911 should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with TieMart, Inc. regarding this incident. If so, please call Mike Martyka at 847-393-7291 x305 from 8:00am-4:00pm Central Time, Monday through Friday.

At TieMart, Inc. we take our responsibilities to protect your account information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Mike Martyka  
President

\* Services marked with an "\*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection and in order to confirm your identity.