



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name>>,

Knit-Rite, Inc., operator of the GoGoHealthy.com, KnitRiteDirect.com, Preggers.com, SmartKnit.com, and Therafirm.com websites (the "Websites"), recently became aware of a security incident potentially affecting the personal information of certain individuals who made a payment card purchase at the Websites. We are providing this notice as a precaution to inform potentially affected customers of the incident and to call their attention to some steps they can take to help protect themselves. We sincerely apologize for any frustration or concern this may cause you.

On October 27, 2015, we were alerted to a potential security incident involving the Websites. Based upon an extensive forensic investigation, it appears that unauthorized individuals installed malicious software on the servers hosting the Websites that was designed to capture user account and payment card information as it is inputted into those systems. We believe that the malware could have compromised certain information (including name, address, website username and password, e-mail address, payment card account number, card expiration date, and payment card security code) of individuals who made a purchase on the Websites between February 17, 2015, and May 27, 2015. According to our records, you made a payment card transaction on the Websites during that timeframe and your information may be affected. Please note that any purchases made using PayPal would not have compromised the payment card information. Furthermore, the Websites do not collect sensitive personal information like Social Security numbers, therefore this type of sensitive information is not at risk.

We take the privacy of personal information seriously, and deeply regret that this incident occurred. We took steps to address and contain this incident promptly after it was discovered, including engaging outside forensic experts to assist us in investigating and remediating the situation. We have removed the malware and have reconfigured and updated the server software to improve the security on our Websites. While we are continuing to review and enhance our security measures, the incident has now been contained and customers can safely use payment cards on the Websites.

We want to make potentially affected customers aware of steps they 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 your credit or debit card immediately.

We are also initiating a password reset for the Websites, which will require you to change your password the next time you login to your account. Please note, if you use the same password on other online accounts, we recommend that you change your password for those accounts as well. You should use different and "strong" password for all accounts/websites. Tips on creating a strong password are available at <http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password> and <http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/>.

Finally, although Social security numbers were not at risk in this incident, we recommend, as a general practice, that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. We are including an "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that

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 at the bottom of this page. 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.

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 at the bottom of this page.

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.

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

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30348
800-685-1111

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion (www.transunion.com)
P.O. Box 1000
Atlanta, GA 30348
877-322-8228

Fraud Alerts: P.O. Box 105069,
Atlanta, GA 30348
Credit Freezes: P.O. Box 105788,
Atlanta, GA 30348

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872