



ELLIS & WINTERS

Writer's E-Mail Address:
alex.pearce@elliswinters.com

Writer's Direct Dial Number:
(919) 865-7019

January 18, 2019

VIA OVERNIGHT MAIL

Office of the Attorney General
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505-0040

Re: Notice of Information Security Incident

Dear Sir or Madam:

I write on behalf of my client, Prime Life Fibers, Inc. ("Prime Life"), the operator of www.weareverincontinence.com, pursuant to Section 51-30-02 of the North Dakota Century Code regarding a data security incident involving the personal information of two (2) North Dakota residents. Prime Life, which is headquartered at 4537 Hillsborough Road, Durham, NC 27705, sells diabetic socks and incontinence supplies such as underwear and bed pads.

On November 20, 2018 Prime Life was notified by a service provider that an unauthorized change had been made to Prime Life's e-commerce website, www.weareverincontinence.com, that resulted in the website being identified as dangerous by certain web browsers. Prime Life immediately began working with its e-commerce and website hosting providers to secure the website and remediate the unauthorized changes, and began an investigation. On December 7, 2018, Prime Life determined that unauthorized code had been inserted on its website that has been known in other instances to allow unauthorized access to information entered on a website by visitors to that website. Prime Life immediately engaged a leading computer forensics firm to determine whether the unauthorized code could have affected customer personal information entered on its website.

On January 8, 2019, the forensics firm determined that the unauthorized code on Prime Life's website had the potential to capture certain payment and contact information for online and telephone orders placed between November 6, 2018 and November 26, 2018. This information may have included customers' first and last name, email address, telephone number, billing address, shipping address, date of birth, and credit or debit card number along with the card's expiration date and card security code. In addition, for

190169

TEL 919.865.7000
FAX 919.865.7010

MAILING ADDRESS

Post Office Box 33550
Raleigh, North Carolina 27636

STREET ADDRESS

4131 Parklake Avenue, Suite 400
Raleigh, North Carolina 27612

www.elliswinters.com

Ellis&Winters LLP

customers who created a new account or logged into an existing account on www.weareverincontience.com when placing an order, the unauthorized code may have also captured their email address and account password. Prime Life is not currently aware of any evidence that this information has been misused.

On January 18, 2019 Prime Life is mailing notification letters to two (2) North Dakota residents who placed online or telephone orders during the time frame noted above via United States First-Class mail in substantially the same form as the enclosed sample letter. Prime Life is offering these individuals twelve months of complimentary identity monitoring services through Kroll. Those services, which are described in the sample letter, include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

To help prevent this type of incident from happening again, Prime Life removed the unauthorized code and has implemented additional security enhancements to its website. In addition, Prime Life reported the incident to the Federal Bureau of Investigation and is actively cooperating with their investigation.

Prime Life takes the security of its customers' personal information very seriously and is committed to protecting that information. If you have any questions or need further information regarding this incident, please contact me at (919) 865-7019 or alex.pearce@elliswinters.com.

Sincerely,



Alexander M. Pearce

Enclosure



<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to tell you about a data security incident involving www.weareverincontinenace.com that may have resulted in unauthorized access to certain of your contact and payment information. We take the privacy and security of our customers' personal information seriously and we deeply regret that this incident occurred.

What Happened?

On November 20, 2018 we were notified that unauthorized changes had been made to our website, www.weareverincontinenace.com. We immediately took steps to secure the website and remediate the unauthorized changes, and began an investigation. On December 7, 2018, we determined that unauthorized code had been inserted on our website that has been known in other instances to allow unauthorized access to information entered on a website. We immediately engaged a leading computer forensics firm to determine whether the unauthorized code could have affected personal information entered on our website.

On January 8, 2019, we determined that the unauthorized code had the potential to capture certain payment and contact information for online and telephone orders placed between November 6, 2018 and November 26, 2018. We are notifying you because you placed an order using the payment card ending in XXXX during that time period.

What Information Was Involved?

We believe the unauthorized code may have captured the following types of information when entered on our website: first and last name, email address, telephone number, shipping address, billing address, date of birth, and credit or debit card number along with that card's expiration date and card security code.

In addition, if you created a new account or logged into an existing account on www.weareverincontience.com when you placed your order, the unauthorized code may have also captured your email address and account password.

What We Are Doing.

Upon discovering the incident, we removed the unauthorized code and took the steps described above. We also reported the incident to the Federal Bureau of Investigation and are actively cooperating with their investigation. To help prevent something like this from happening again in the future, we have implemented enhanced security measures on our website.

Although we are not aware of any evidence that your personal information has been misused, we have also secured the services of Kroll to provide identity monitoring at no cost to you for twelve months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until April 18, 2019 to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive identity monitoring services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

What You Can Do.

We recommend that you review the enclosed "Additional Resources" included with this letter. The enclosure describes additional steps you can 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.

In addition, if you created an account on www.weareverincontience.com or logged into an existing www.weareverincontience.com account when you placed your order, you should change the password for that account and any other online accounts for which you use the same email address and password.

For More Information.

If you have questions, please call 1-866-775-4209, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,



Robert F. Deerin,
President, Prime Life Fibers, Inc.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL RESOURCES

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax

www.equifax.com
Phone: 1-800-685-1111
PO Box 740241, Atlanta, GA 30374

Experian

www.experian.com
Phone: 1-888-397-3742
PO Box 2104, Allen, TX 75013

TransUnion

www.transunion.com
Phone: 1-800-888-4213
PO Box 2000, Chester, PA 19022

Fraud Alerts:

PO Box 740256, Atlanta, GA 30374

Fraud Alerts and Security Freezes:

PO Box 9554, Allen, TX 75013

Fraud Alerts and Security Freezes:

PO Box 2000, Chester, PA 19022

Credit Freezes

PO Box 1005788, Atlanta, Ga 30348

Free Credit Report. Under the Fair Credit Reporting Act ("FCRA"), you are entitled to obtain a copy of your credit report at your request, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fair Credit Reporting Act. In addition to obtaining a copy of your credit report, you have the following rights under the FCRA:

- You are entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company.
- You are entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information and may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Fraud Alert. You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above.

Security Freeze. You have the ability to place a security freeze on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well):

- (1) full name, with middle initial and any suffixes;
- (2) Social Security number;
- (3) date of birth;
- (4) current address and any previous addresses for the past five years;
- (5) proof of current address (e.g., recent utility or telephone bill or bank or insurance statement)
- (6) a legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.)
- (7) if you are a victim of theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency or the Registry of Motor Vehicles concerning identity theft.

For more information and instructions on placing a fraud alert or a security freeze, contact the FTC or the credit reporting agencies above.

Reporting of Identity Theft and Obtaining a Police Report. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. Contact information for the FTC is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland and North Carolina residents, you may contact and obtain information from your state attorney general at:

Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 or 1-919-716-6400.

For Iowa residents: You are advised to report suspected identity theft to local law enforcement and the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report relating to this incident and, if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.