

Interstitial Cystitis Network

www.ic-network.com

PO Box 2159

Healdsburg, CA 95448

Toll Free - 800.928.7496

Direct - 707.538.9442

October 26, 2015

Dear ICN Customer.

It is with a heavy heart that I share with you that the ICN Mail Order Center (www.icnsales.com) has experienced a security breach which may have compromised your personal information (i.e. your name, address, credit or debit card number, expiration date and CVV code).

We first learned of a possible breach when two customers contacted our office to report that their credit card information may have been compromised. In both cases, they first experienced a fraudulent charge on Facebook. We immediately performed a security review of our server and are confident that the breach did not occur in our offices or the systems that we directly maintain. Our investigation revealed that the breach occurred through the use of a password stolen from one of our vendors.

The ICN does not store any credit card information once an order has been placed. ICN employees cannot review your credit card number after an order has been placed. In this event, they captured order information as it was being placed. Once we discovered the intrusion, our store was shut down until files were reviewed, corrected and all passwords were changed.

Date of the Breach

The information we have indicates that transactions between April 6, 2015 and October 1, 2015 may have been compromised.

Information Potentially Compromised

- Your Name, Address, Phone & Email address
- Your Payment Information / CC, Expiry Date, CVV code

What You Should Do

If you used a debit card to make a purchase on our site, we recommend that you immediately contact your bank and review your transaction history. Experts suggest that debit cards should never be used for online purchases and that bank accounts attached to the compromised cards be changed immediately.

If you used a credit card to make a purchase on our site, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. Credit cards companies have strong security measures and usually catch unusual expenditures. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state Attorney General, or the Federal Trade Commission.

To file a complaint with the Federal Trade Commission, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281,

Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below.

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834
---	--	--

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://annualcreditreport.com>.

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$5 to place, lift, or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (877-438-4338).

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491

North Carolina residents may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

While I am relieved that our server integrity was not forcefully breached, I feel violated that our website, which serves patients in pain and distress, was targeted. They are criminals and they have no conscience. I apologize for any inconvenience that this may cause you. My personal credit card was also compromised. I feel your frustration and anger. If you have any questions or comments, please don't hesitate to contact me directly at (707) 538-9442.

Sincerely Yours,

Jill H. Osborne
President & Founder
jill@ic-network.com